IN THE CIRCUIT COURT FOR BALTIMORE CITY, MARYLAND

JANE DOE,
c/o Salsbury Sullivan, LLC
100 N. Charles Street, Suite 900
Baltimore, MD 21201
On behalf of herself and all others similarly situated,

Plaintiff,

v.

THE UNIVERSITY OF MARYLAND MEDICAL SYSTEM CORPORATION,
22 S. Greene St.
Baltimore, Maryland 21201

Defendant.

Case No. 24C23000574

FIRST AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all other current Citizens of the state of Maryland similarly situated ("Class Members"), brings suit against Defendant University of Maryland Medical System Corporation d/b/a University of Maryland Medical Center ("UMMC" or "Defendant"), and upon personal knowledge as to Plaintiff's own conduct and on information and belief as to all other matters based upon investigation by counsel, alleges as follows:

INTRODUCTION

1. This case arises from Defendant's systematic violation of the medical privacy rights of its patients, exposing highly sensitive personal information to third parties without those patients' knowledge or consent.

2. Defendant assures visitors to its website that "[w]e are required by law to maintain the privacy and security of your protected health information" and that "[w]e will let

you know promptly if a breach occurs that may have compromised the privacy or security of your information."[1] Likewise, Defendant promises patients that "we never share your information" for "[m]arketing purposes" or for the "[s]ale of your information" unless "you give us written permission."[2] Contrary to these assurances, however, Defendant has not followed these policies, nor the law prohibiting such disclosures.

3. At all relevant times, Defendant disclosed information about its patients—including their status as patients, their physicians, their medical treatments, the hospitals they visited, and their personal identities—to Facebook, Google, and other third parties without its patients' knowledge, authorization, or consent.

4. Defendant disclosed this protected health information through the deployment of various digital marketing and automatic data collection tools embedded on its websites that purposefully and intentionally intercept and transmit patients' personal health information to third parties who exploit that information for advertising purposes. Defendant's use of these tools caused Plaintiff's and Class Members' personally identifiable information and the contents of their communications exchanged with Defendant to be automatically provided to third parties in violation of those patients' reasonable expectations of privacy, their rights as patients, their rights as citizens of Maryland, and both the express and implied promises of Defendant.

5. Defendant's conduct in disclosing such protected health information about its patients to Facebook and other third parties without notice or consent violates Maryland law, including Md. Code Ann. CJP § 10-402 (Wiretapping), HG § 4-302 (Confidentiality of Medical Records; Disclosure), CL § 14-3502 (Protection of Customer's Personal Information), and CL § 14-305 (Reasonable Security Procedures and Practices).

---

[1] https://www.umms.org/ummc/about/policies/privacy-policy
[2] https://www.umms.org/ummc/about/policies/privacy-policy

6. On behalf of herself and all similarly situated, current citizens of the state of Maryland, Plaintiff seeks an order enjoining Defendant from further unauthorized disclosures of her personal information; awarding liquidated damages in the amount of $1,000 per violation, attorney's fees and costs; and granting any other preliminary or equitable relief the Court deems appropriate.

PARTIES TO THE ACTION

7. Defendant University of Maryland Medical System Corporation d/b/a University of Maryland Medical Center is a Maryland corporation that operates acute care hospitals, with its headquarters and principal place of business at 250 West Pratt Street, 24th Floor, Baltimore, Maryland, 20201. Defendant provides health services, coordinated across its downtown and midtown Baltimore hospital campuses and multiple community locations, including primary care and urgent care centers. Defendant also manages multiple specialty practices, including the R Adams Cowley Shock Trauma Center, the University of Maryland Mariene and Stewart Greenebaum Comprehensive Cancer Center, the University of Maryland Division of Transplantation, the University of Maryland Heart and Vascular Center, the University of Maryland Center for Diabetes and Endocrinology, and the University of Maryland Center for Pulmonary Health.[3]

8. Plaintiff, Jane Doe, is a Maryland citizen residing in Prince George's County, and has been a patient at the UM Laurel Medical Center[4], and thus also a patient of Defendant.

[3] https://www.umms.org/ummc/-/media/files/umms/about-us/member-hospitals/fact-sheets/ummc-fact-sheet-2020.pdf?upd=20201229173508
[4] https://www.umms.org/capital/locations/um-laurel-medical-center

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to Md. Code Ann., Cts. & Jud. Proc. § 4-402(d)(1)(ii).

10. This Court has personal jurisdiction over Defendant because it regularly conducts business throughout Maryland has its principal place of business at 250 West Pratt Street, 24th Floor, Baltimore, Maryland, 20201. *See* Md. Code Ann., Cts. & Jud. Proc. §§ 6-102(a), 6-103.

11. Venue is appropriate in this Court pursuant to Md. Code Ann., Cts. & Jud. Proc. § 6-201(a) because Defendant maintains its principal office in Baltimore, Maryland and a substantial part of the acts and omissions giving rise to this lawsuit occurred in Baltimore, Maryland.

FACTUAL BACKGROUND

A. Defendant routinely disclosed the protected health information of its patients to third parties including Facebook.

12. Plaintiff Jane Doe is a patient of Defendant who has received treatment from UMMC.

13. As Maryland law has long recognized, physicians have a duty to maintain the confidentiality of patients' medical records. HG § 4-302(a).

14. Medical patients in Maryland such as Jane Doe have a legal interest in preserving the confidentiality of their communications with healthcare providers.

15. Patients also have reasonable expectations of privacy that their personally identifiable information and communications will not be disclosed to third parties by Defendant without their express written consent and authorization.

16. As a health care provider, Defendant has fiduciary, common law, and statutory duties to protect the confidentiality of patient information and communications.

17. Defendant expressly and impliedly promises patients that it will maintain and protect the confidentiality of personally identifiable patient information and communications.

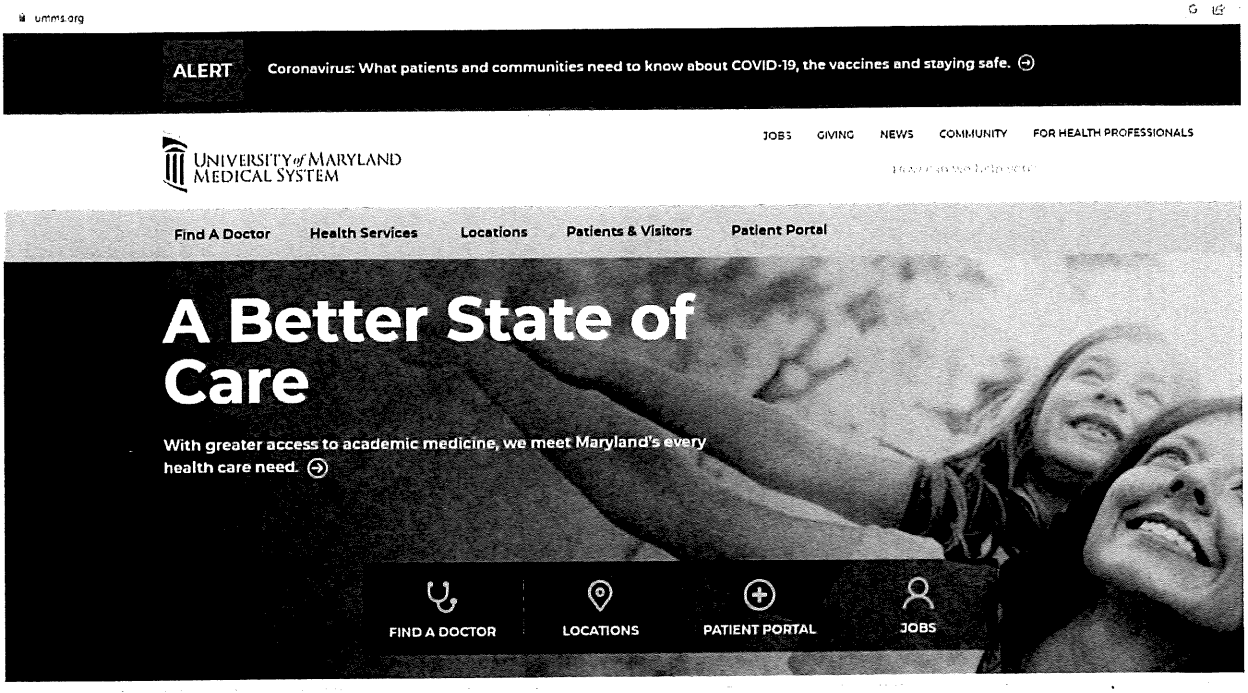
18. Defendant operates websites for patients, including https://www.umms.org/ummc.

19. Defendant's websites are designed for interactive communication with patients, including scheduling appointments, searching for physicians, paying bills, requesting medical records, learning about medical issues and treatment options, and joining support groups.

20. Notwithstanding patients' reasonable expectations of privacy, Defendant's legal duties of confidentiality, and Defendant's express promises to the contrary, Defendant disclosed the contents of patients' communications and protected healthcare information via automatic data collection mechanisms embedded in the websites operated by Defendant without patients' knowledge, authorization, or consent.

21. Defendant encourages patients to use digital tools on its websites to seek and receive health care services. Plaintiff and Class Members provided their private information to Defendant's website with the reasonable understanding that Defendant would secure and preserve the confidentiality of that information.

22. The home page of Defendant's website is designed for use by patients. The home page provides patients with tools to seek medical treatment, such as "Find A Doctor," "Health Services, and "Patient Portal."



23. Defendant also maintains a patient portal, which allows patients to make appointments, access medical records, view lab results, and exchange communications with health care providers. Plaintiff's and Class Members' communications with Defendant included their sign-up and subsequent logins to Defendant's patient portal. Source code on Defendant's website causes these communications to be intercepted and disclosed to multiple third parties, including Google.

24. Plaintiff and Class Members provided their private information to Defendant's website with the reasonable understanding that Defendant would secure and preserve the confidentiality of that information.

25. Notwithstanding patients' reasonable expectations of privacy, Defendant's legal duties of confidentiality, and Defendant's express promises to the contrary, Defendant disclosed the contents of patients' communications and protected healthcare information via automatic data collection mechanisms embedded in the websites operated by Defendant without patients'

knowledge, authorization, or consent. In doing so, Defendant systematically violated the medical privacy rights of its patients by causing the unauthorized disclosure of patient communications to be transmitted to Facebook, Google, and other third-party marketing companies.

26. Defendant encourages patients to use digital tools on its websites to seek and receive health care services. Plaintiff and Class Members provided their private information to Defendant's website with the reasonable understanding that Defendant would secure and preserve the confidentiality of that information.

27. The private information provided by Plaintiff and Class Members has been—and likely will be—further disseminated to additional third parties utilizing the information for retargeting.

28. While Defendant intentionally incorporated tracking tools onto its website, Defendant never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications with Facebook, Google, and other third parties. As a result, Plaintiff and Class Members were unaware that their private information was being surreptitiously transmitted to third parties when they visited Defendant's website.

29. By design, none of the tracking mechanisms employed by Defendant are visible to patients visiting Defendant's website.

30. Defendant did not warn or otherwise disclose to Plaintiff and Class Members that Defendant bartered their confidential medical communications to Facebook, Google, and other third parties for marketing purposes.

31. Plaintiff and Class Members never consented, agreed, or otherwise authorized Defendant to disclose their confidential medical communications, particularly not beyond the

limits of Defendant's express promises to protect the confidentiality of Plaintiff's and Class Members' private information.

32. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiff's and Class Members' status as patients;

b. Plaintiff's and Class Member's communications with Defendant via its website;

c. Plaintiff's and Class Members' use of Defendant's patient portal;

d. Plaintiff's and Class Member's searches for information regarding specific medical conditions and treatments, their medical providers, and their physical location.

33. Defendant interfered with Plaintiff's and Class Members' privacy rights when it implemented technology (including the Meta Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential information to Facebook, Google, and other third parties.

34. Defendant also breached its obligations to patients in multiple other ways, including (1) failing to obtain their consent to disclose their private information to Facebook and other third parties, (2) failing to adequately review its marketing programs and web-based technology to ensure its website was safe and secure, (3) failing to remove or disengage software code that was known and designed to share patients' private information with third parties, (4) failing to take steps to block the transmission of Plaintiff's and Class Members' private information to Facebook and other third-party advertising companies, (5) failing to warn Plaintiff and Class Members that Defendant was routinely bartering their private information to Facebook via the Meta Pixel, and (6) otherwise ignoring Defendant's common and statutory obligations to protect the confidentiality of patient's protected health information.

35. Plaintiff and Class Members have suffered injury because of Defendant's conduct. Their injuries include invasion of privacy and the continued and ongoing risk of irreparable harm from the disclosure of their most sensitive and personal information.

B. The nature of Defendant's unauthorized disclosure of patients' health care information.

36. Defendant's disclosures of patients' personal healthcare information occurred because Defendant intentionally deployed source code on the websites it operates, including www.umms.org, that caused patients' personally identifiable information (as well as the exact contents of their communications) to be transmitted to third parties.

37. By design, these third parties receive and record the exact contents of patient communications before the full response from Defendant to patients has been rendered on the screen of the patient's computer device and while the communication between Defendant and the patient remains ongoing.

38. For example, when Plaintiff or a Class Member accessed Defendant's website pages hosting the Meta Pixel, the Meta Pixel software directed their browsers to send a message to Facebook's servers. The information that Defendant sent to Facebook included the private information that Plaintiff and Class Members communicated to Defendant's website, such as the type of medical appointment the patient made, the date, and the specific doctor the patient was seeing.

39. Such private information allows third-party advertising companies like Facebook to determine that a specific patient was seeking a specific type of confidential medical treatment. This kind of disclosure also allows Facebook to reasonably infer that a specific patient was being treated for specific types of medical conditions, such as cancer.

40. Websites like those maintained by Defendant are hosted by a computer server through which the business in charge of the website exchanges and communicates with internet users via their web browsers.

41. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with internet users via a client device, such as a computer, tablet, or smart phone, via the client device's web browser.

42. Web browsers are software applications that allow users to exchange electronic communications over the internet.

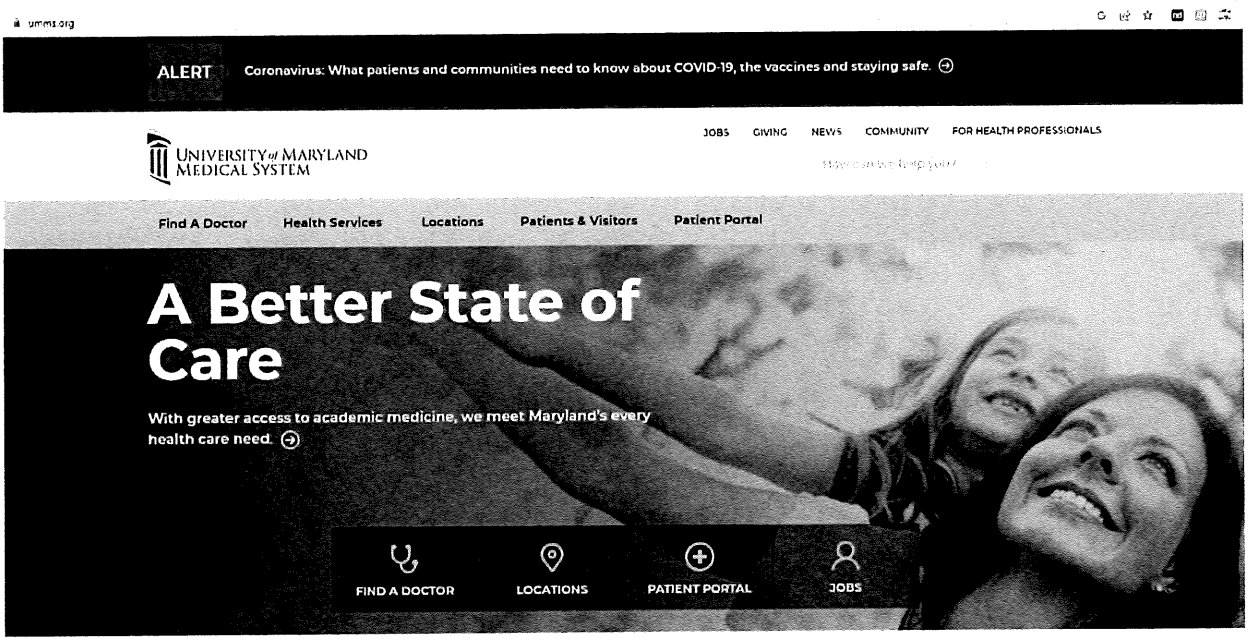
43. Each exchange of an electronic communication over the internet typically consists of an HTTP request from a client device and an HTTP response from a server. When a user types a URL into a web browser, for example, the URL is sent as an HTTP request to the server corresponding to the web address, and the server then returns an HTTP response that consists of a web page to render in the client device's web browser.

44. In addition to specifying the URL, HTTP requests can also send data to the host server, including users' cookies. Cookies are text files stored on client devices to record data, often containing sensitive, personally identifiable information.

45. In turn, HTTP responses may consist, among other things, of a web page, another kind of file, text information, or error codes.

46. A web page consists primarily of "Markup" and "Source Code." The markup of a web page comprises the visible portion of that web page. Markup is displayed by a web browser in the form of words, paragraphs, images, and videos displayed on a users' device screen. The source code of a web page is a set of instructions that commands the browser to take certain actions, either when the web page loads or when a specified event triggers the code.

47. For example, typing https://www.umms.org/ into a browser sends an HTTP request to Defendant's website, which returns a HTTP response in the form of the home page of Defendant's website:



48. Source code is not visible on the client device's screen, but it may change the markup of a webpage, thereby changing what is displayed on the client device's screen. Source code may also execute a host of other programmatic instructions, including commanding a web browser to send data transmissions in the form of HTTP requests to the website's server, or, as is the case with Defendant's website, to third parties via pixels.

49. For example, Defendant's website includes software code that transmits HTTP requests *directly* to Facebook, including patients' private health information, every time a patient interacts with a page on its website.

50. The basic command that web browsers use to exchange data and user communications is called a GET request.[5] For example, when a patient types "heart failure treatment" into the search box on Defendant's website and hits 'Enter,' the patient's web browser makes a connection with the server for Defendant's website and sends the following request: "GET search/q=heart+failure+treatment."

51. When a server receives a GET request, the information becomes appended to the next URL (or "Uniform Resource Locator") accessed by the user. For example, if a patient enters "respiratory problems" into the query box of a website search engine, and the search engine transmits this information using a GET request method, then the words "respiratory" and "problems" will be appended to the query string at the end of the URL of the webpage showing the search results.

52. The other basic transmission command utilized by web browsers is POST, which is typically employed when a user enters data into a form on a website and clicks 'Enter' or some other form of submission button. POST sends the data entered in the form to the server hosting the website that the user is visiting.

53. In response to receiving a GET or POST command, the server for the website with which the user is exchanging information will send a set of instructions to the web browser and command the browser with source code that directs the browser to render the website's responsive communication.

54. Once the initial connection is made between a user and a website, the communications commence and continue between the parties in a bilateral fashion until the user leaves the website.

[5] https://www.w3schools.com/tags/ref_httpmethods.asp

55. Unbeknownst to users, however, the website's server may also transmit the user's communications to third parties via third party tracking tools. Indeed, Google warns website developers and publishers that installing its ad tracking software on webpages employing GET requests will result in users' personally identifiable information being disclosed to Google.[6]

56. Third parties (such as Facebook and Google) may use the information they receive to track user data and communications for marketing purposes.

57. In many cases, third-party marketing companies acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a tracking pixel, a web-bug, or a web beacon. These tracking pixels are tiny and are purposefully camouflaged to remain invisible to users.

58. Tracking pixels can be placed directly on a web page by a developer, or they can be funneled through a "tag manager" service to make the invisible tracking run more efficiently and to further obscure the third parties to whom users' personally identifiable data and communications are transmitted without their knowledge or consent.

59. Tag managers are simple enough that non-programmers can use them to deploy and remove digital tracking tools from web-properties with just the click of a few buttons.

60. Defendant deploys Google Tag Manager on its website through an "iframe," a nested "frame" that exists within the Defendant's website that is, in reality, an invisible window through which Defendant funnels tracking pixels for third parties to secretly acquire the content of patient communications without any knowledge, consent, authorization, or further action of patients.

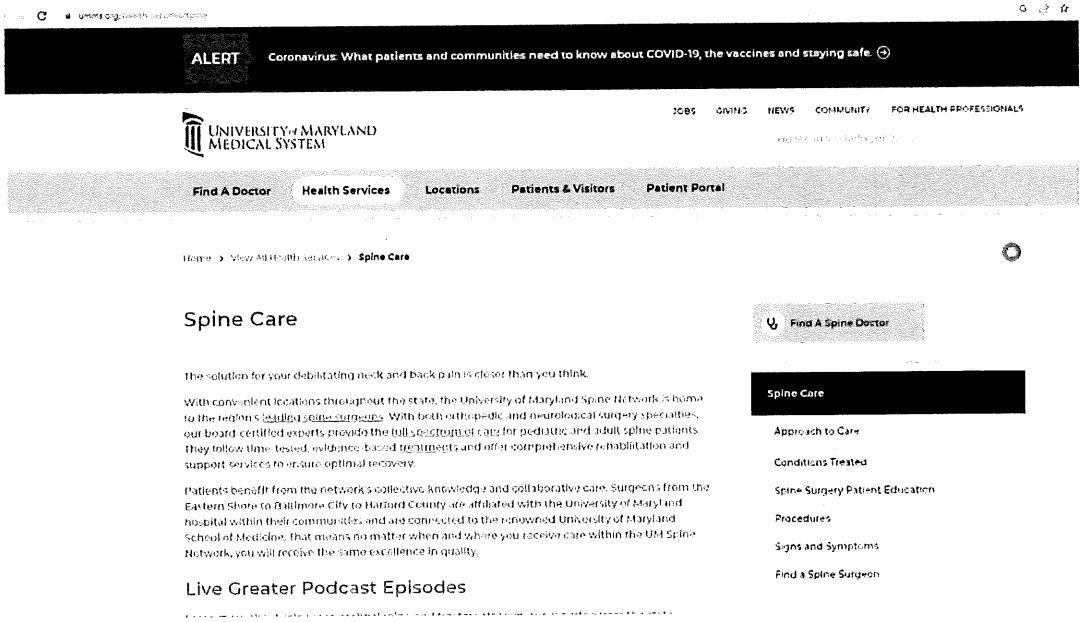
[6] https://support.google.com/platformspolicy/answer/6156630?hl=en

61. Defendant's Google Tag Manager source code is designed to be invisible. The source code employed by Defendant specifies an "iframe" with a height of 0, width of 0, display of none, and visibility hidden.

62. Defendant then funnels invisible 1x1 tracking pixels or web-bugs through this purposely invisible iframe to help third parties track, acquire, and record patient data and communications.

63. By design, none of the tracking is visible to patients visiting Defendant's website.

64. These tracking pixels can collect dozens of data points about individual website users who interact with a website. For example, when a patient clicks through Defendant's website to the page describing Defendant's "spine" services at https://www.umms.org/health-services/spine, the source code deployed on Defendant's website causes personally identifiable data and the content of patient communications to be transmitted to third parties:



65. By design, the transmission of patient data to third parties occurs before Defendant's responsive communications about "spine care" services have been delivered in full to the patient.

66. In addition to the Google Tag Manager, other source code is also placed on Defendant's website, resulting in the interception and transmission of patient personal health information to multiple third parties.

67. A web site developer who chooses to deploy third-party source code, like a tracking pixel, on their website must include the third-party source code directly in their website for every third party they wish to send user data and communications. This source code operates invisibly in the background when users visit a site employing such code.

68. For example, one of the world's most prevalent tracking pixels, called the Meta Pixel, is provided by Facebook.

69. Tracking pixels such as the Meta Pixel tool allow Defendant and Facebook to secretly track, intercept, record, and transmit every patient communication made on Defendant's website. When patients visit Defendant's website, unbeknownst to them, the web page displayed on the patient's browser includes the Meta Pixel as embedded code, which is not visible to patients or other visitors to Defendant's website. This code is triggered when a patient or visitor interacts with the web page. Each time the Meta Pixel is triggered, the software code is executed and sends patient's private information directly to Facebook.

70. The Meta Pixel and similar tracking pixels act like a physical wiretap on a phone. Like a physical wiretap, pixels do not appear to alter the function of the communication device on which they surreptitiously installed. Instead, these pixels lie in wait until they are triggered by an event, at which time they effectively open a channel through the website funnels data

about users and their actions to third parties via a hidden HTTP request that is never shown to or agreed to by the user.

71. For example, a patient can trigger an HTTP request by interacting with the search bar on Defendant's website by typing a term such as "breast cancer" into the search bar and then hitting enter. Defendant's server in turn sends an HTTP response, which results in the search results being displayed.

72. This is not the only HTTP request, however, that is created by a patient's interaction with Defendant's website. In fact, at the very same time the web page is instructed to send an HTTP request to Defendant requesting search results, the hidden source code, acting as a tap, is triggered, such that Defendant's website is also instructed to send an HTTP request directly to Facebook, Google, and other third parties, informing them of the patient's exact search and the patient's personally identifiable information.

C. Tracking pixels provide third parties with a trove of personally identifiable information.

73. Tracking pixels are especially pernicious because they result in the disclosure of a variety of personally identifiable information.

74. For example, an IP address is a numerical identifier that identifies each computer connected to the internet. IP addresses are used to identify and route communications on the internet. IP addresses of individual users are used by internet service providers, websites, and tracking companies to facilitate and track internet communications and content. IP addresses also offer advertising companies like Facebook a unique and semi-persistent identifier across devices—one that has limited privacy controls.[7]

[7] https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/

75. Because of their uniquely identifying characteristics, IP addresses are considered personally identifiable information. 45 CFR § 164.514. Tracking pixels can (and typically do) collect website visitors' IP addresses.

76. Likewise, internet cookies also provide personally identifiable information. 45 CFR § 164.514.

77. In the early years of the internet, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early internet paid for ads to be placed on specific web pages based on the type of content displayed.

78. Computer programmers eventually developed 'cookies'—small text files that web servers can place on a user's browser and computer when a user's browser interacts with a website server. Eventually some cookies were designed to acquire and record an individual internet user's communications and activities on websites across the internet.

79. Cookies are designed to operate as a means of identification for internet users. Advertising companies like Facebook and Google have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell targeted advertising that is customized to a user's personal communications and browsing history. To build individual profiles of internet users, third party advertising companies assign each user a unique (or a set of unique) identifiers to each user.

80. Cookies are considered personally identifiable information, and tracking pixels can collect cookies from website visitors.

81. In general, cookies are categorized by (1) duration and (2) party.

82. There are two types of cookies classified by duration.

83. "Session cookies" are placed on a user's computing device only while the user is navigating the website that placed and accesses the cookie. The user's web browser typically deletes session cookies when the user closes the browser.

84. "Persistent cookies" are designed to survive beyond a single internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user's internet communications for years and over dozens or even hundreds of websites. Persistent cookies are also called "tracking cookies."

85. Cookies are also classified by the party that uses the collected data.

86. "First-party cookies" are set on a user's device by the website with which the user is exchanging communications. First-party cookies can be helpful to the user, server, and/or website to assist with security, login, and functionality.

87. "Third-party cookies" are set on a user's device by website servers other than the website or server with which the user is exchanging communications. For example, the same patient who visits Defendant's website will also have cookies on their device from third parties, such as Facebook and Google. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

88. Data companies like Facebook have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell advertising that is customized to a user's communications and habits. To build individual profiles of internet users, third party data companies assign each user a unique identifier or set of unique identifiers.

89. Traditionally, first-party and third-party cookies were kept separate. An internet security policy known as the same-origin policy required web browsers to prevent one web server from accessing the cookies of a separate web server. For example, although Defendant can deploy source code that uses Facebook third-party cookies to help Facebook acquire and record a patient's communications, Defendant is not permitted direct access to Facebook third-party cookie values. The reverse *was* also true: Facebook was not provided direct access to the values associated with first-party cookies set by companies like Defendant. But Data companies have designed a way to hack around the same-origin policy so that third-party data companies like Facebook can gain access to first-party cookies.

90. JavaScript source code developed by third party data companies and placed on a webpage by a developer such as Defendant can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to the third-party data company. This technique is known as "cookie synching," and it allows two cooperating websites to learn each other's cookie identification numbers for the same user. Once the cookie synching operation is completed, the two websites can exchange any information that they have collected and recorded about a user that is associated with a cookie identifier number. The technique can also be used to track an individual who has chosen to deploy third-party cookie blockers.

91. In effect, cookie synching is a method through which Facebook, Google, and other third-party marketing companies set and access third-party cookies that masquerade as first-party cookies. By designing these special third-party cookies that are set for first-party websites, Facebook and Google hack their way around any cookie blockers that users set up to stop their tracking.

92. The Facebook cookie used for cookie synching is named _fbp.

93. Defendant engages in cookie synching with Facebook, Google, and other third parties.

94. Defendant' cookie disclosures include the deployment of cookie synching techniques that cause the disclosure of the first-party cookie values that Defendant assigns to patients to also be made to third parties.

95. Defendant uses and causes the disclosure of patient cookie identifiers with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments

96. A third type of personally identifiable information is what data companies refer to as a "browser-fingerprint." A browser-fingerprint is information collected about a computing device that can be used to identify a specific device.

97. These browser-fingerprints can be used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data. As Google explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."[8] The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.[9] Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.[10]

[8] https://www.blog.google/products/chrome/building-a-more-private-web/
[9] https://pixelprivacy.com/resources/browser-fingerprinting/
[10] https://www.blog.google/products/chrome/building-a-more-private-web/

98. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[11]

99. Browser-fingerprints are considered personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors.

100. Defendant uses and causes the disclosure of data sufficient for third parties to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments.

101. A fourth kind of personally identifiable information protected by law against disclosure are unique user identifiers (such as Facebook's "Facebook ID") that permit companies like Facebook to quickly and automatically identify the personal identity of its user across the internet whenever the identifier is encountered. A Facebook ID is an identifiable number string that is connected to a user's Facebook profile.[12] Anyone with access to a user's Facebook ID can locate a user's Facebook profile.[13]

102. Unique identifiers such as a person's Facebook ID are likewise capable of collection through pixel trackers.

103. Each of the individual data elements described above is personally identifiable on their own. However, Defendant's disclosures of such personally identifiable data elements do not occur in a vacuum. The disclosures of the different data elements are tied together and, when taken together, these data elements are even more accurate in identifying individual patients, particularly when disclosed to data companies such as Facebook, Google, and other internet marketing companies that expressly state that they use such data elements to identify individuals.

---

[11] https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/
[12] https://www.facebook.com/help/211813265517027
[13] https://smallseotools.com/find-facebook-id/

D. Facebook's Business Model: Exploiting Users' Personal Data to Sell Advertising

104. Facebook, a social media platform founded in 2004 and today operated by Meta Platforms, Inc., was originally designed as a social networking website for college students.

105. Facebook describes itself as a "real identity" platform.[14] This means that users are permitted only one account and must share "the name they go by in everyday life."[15] To that end, Facebook requires users to provide their first and last name, along with their birthday, telephone number and/or email address, and gender, when creating an account.[16]

106. In 2007, realizing the value of having direct access to millions of consumers, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming this service to be a "completely new way of advertising online," that would allow "advertisers to deliver more tailored and relevant ads."[17] Facebook has since evolved into one of the largest advertising companies in the world.[18] Facebook can target users so effectively because it surveils user activity both on and off its website through the use of tracking pixels.[19] This allows Facebook to make inferences about users based on their interests, behavior, and connections.[20]

107. Today, Facebook provides advertising on its own social media platforms, as well as other websites through its Facebook Audience Network. Facebook has more than 2.9 billion users.[21]

108. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal

---

[14] https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701#:~:text=Facebook%20said%20in%20its%20most,of%20them%20than%20developed%20ones.
[15] https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/
[16] https://www.facebook.com/help/406644739431633
[17] https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/
[18] https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/
[19] https://www.facebook.com/business/help/742478679120153?id=120537668283214 2
[20] https://www.facebook.com/business/ads/ad-targeting
[21] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code. Facebook employs algorithms, powered by machine learning tools, to determine what advertisements to show users based on their habits and interests, and utilizes tracking software such as the Meta Pixel to monitor and exploit users' habits and interests.

109. Tracking information about users' habits and interests is a critical component of Facebook's business model because it is precisely this kind of information that allows Facebook to sell advertising to its customers. Facebook uses plug-ins and cookies to track users' browsing histories when they visit third-party websites. Facebook then compiles these browsing histories into personal profiles which are sold to advertisers to generate profits.

110. Facebook offers several advertising options based on the type of audience that an advertiser wants to target. Those options include targeting "Core Audiences," "Custom Audiences," "Look Alike Audiences," and even more granulated approaches within audiences called "Detailed Targeting." Each of Facebook's advertising tools allow an advertiser to target users based, among other things, on their personal data, including geographic location, demographics (e.g., age, gender, education, job title, etc.), interests, (e.g., preferred food, movies), connections (e.g., particular events or Facebook pages), and behaviors (e.g., purchases, device usage, and pages visited). This audience can be created by Facebook, the advertiser, or both working in conjunction.

111. Ad Targeting has been extremely successful due to Facebook's ability to target individuals at a granular level. For example, among many possible target audiences, "Facebook offers advertisers 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users

who 'prefer high-value goods in Mexico.'"[22] Aided by highly granular data used to target specific users, Facebook's advertising segment quickly became Facebook's most successful business unit, with millions of companies and individuals utilizing Facebook's advertising services.

E. Facebook's Meta Pixel tool allows Facebook to track the personal data of individuals across a broad range of third-party websites.

112. To power its advertising business, Facebook uses a variety of tracking tools to collect data about individuals, which it can then share with advertisers. These tools include software development kits incorporated into third-party applications, its "Like" and "Share" buttons (known as "social plug-ins"), and other methodologies, which it then uses to power its advertising business.

113. One of Facebook's most powerful tools is called the "Meta Pixel." Once a third-party like Defendant installs the Meta Pixel on its website, by default it begins sending user information to Facebook automatically.[23]

114. The Meta Pixel is a snippet of code embedded on a third-party website that tracks users' activities as users navigate through a website.24 Once activated, the Meta Pixel "tracks the people and type of actions they take."25 Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information that users input into a website.26 The Meta Pixel code works by sending Facebook a detailed log of a user's interaction with a website such as clicking on a product or running a search via a query box. The Meta Pixel also captures

[22] https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html
[23] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector
[24] https://developers.facebook.com/docs/meta-pixel/
[25] https://www.facebook.com/business/goals/retargeting
[26] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

information such as what content a user views on a website or how far down a web page they scrolled.[27]

115. When someone visits a third-party website page that includes the Meta Pixel code, the Meta Pixel code is able to replicate and send the user data to Facebook through a separate (but simultaneous) channel in a manner that is undetectable by the user.[28] This information is disclosed to Facebook regardless of whether a user is logged into their Facebook account at the time.

116. The information Meta Pixel captures and discloses to Facebook includes a referrer header (or "URL"), which includes significant information regarding the user's browsing history. When users enter a URL address into their web browser using the 'http' web address format, or click hyperlinks embedded on a web page, they are actually telling their web browsers (the client) which resources to request and where to find them. Thus, the URL provides significant information regarding a user's browsing history, including the identifiable information of the internet user and the web server, as well as the name of the web page and the search terms that the user used to find it.

117. These search terms and the resulting URLs divulge a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's own platform. In this manner, Facebook tracks users browsing histories on third-party websites, and compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue.[29]

118. For example, if Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added an item

---

[27] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector
[28] *See, e.g., In re Facebook, Inc. Internet Tracking Litigation,* 956 F.3d 589, 596 (9th Cir. 2020) (explaining functionality of Facebook software code on third-party websites).
[29] *In re Facebook*, 956 F.3d at 596.

to their cart, as well as what they purchased. Along with this data, Facebook also receives personally identifiable information like IP addresses, Facebook IDs, user agent information, device identifiers, and other data. All this personally identifiable data is available each time the Meta Pixel forwards a user's interactions with a third-party website to Facebook's servers. Once Facebook receives this information, Facebook processes it, analyzes it, and assimilates it into datasets like its Core Audiences and Custom Audiences. Facebook can then sell this information to companies who wish to display advertising for products similar to what the user looked at on the original shopping website.

119. These communications with Facebook happen silently, without users' knowledge. By default, the transmission of information to Facebook's servers is invisible. Facebook's Meta Pixel allows third-party websites to capture and send personal information a user provides to match them with Facebook or Instagram profiles, even if they are not logged into Facebook at the time.[30]

120. In exchange for installing its Meta Pixel, Facebook provides website owners like Defendant with analytics about the ads they've placed on Facebook and Instagram and tools to target people who have visited their website.[31] The Meta Pixel collects data on website visitors regardless of whether they have Facebook or Instagram accounts.[32]

121. Facebook can then share analytic metrics with the website host, while at the same time sharing the information it collects with third-party advertisers who can then target users based on the information collected and shared by Facebook.

122. Facebook touted Meta Pixel (which it originally called "Facebook Pixel") as "a

[30] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector
[31] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
[32] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

new way to report and optimize for conversions, build audiences and get rich insights about how people use your website."[33] According to Facebook, the Meta Pixel is an analytics tool that allows business to measure the effectiveness of their advertising by understanding the actions people take on their websites."[34]

123. Facebook warns web developers that its Meta Pixel enables Facebook "to match your website visitors to their respective Facebook User accounts."[35]

124. Facebook recommends that its Meta Pixel code be added to the base code on every website page (including the website's persistent header) to reduce the chance of browsers or code from blocking Pixel's execution and to ensure that visitors will be tracked.[36]

125. Once Meta Pixel is installed on a business's website, the Meta Pixel tracks users as they navigate through the website and logs which pages are visited, which buttons are clicked, the specific information entered in forms (including personal information), as well as "optional values" set by the business website.[37] Facebook builds user profiles on users that include the user's real name, address, location, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, such as IP addresses and the Facebook ID. Meta Pixel tracks this data regardless of whether a user is logged into Facebook.

126. Facebook tracks non-Facebook users through its widespread internet marketing products and source code and its CEO, Mark Zuckerberg, conceded that the company maintains "shadow profiles" on nonusers of Facebook.[38]

---

[33] https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/
[34] https://www.oviond.com/understanding-the-facebook-pixel
[35] https://developers.facebook.com/docs/meta-pixel/get-started
[36] https://developers.facebook.com/docs/meta-pixel/get-started
[37] https://developers.facebook.com/docs/meta-pixel/
[38] https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/

127. For Facebook, the Meta Pixel tool embedded on third-party websites acts as a conduit for information, sending the information it collects to Facebook through scripts running in a user's internet browser, similar to how a "bug" or wiretap can capture audio information. The information is sent in data packets, which include personally identifiable data.

128. For example, the Meta Pixel is configured to automatically collect "HTTP Headers" and "Pixel-specific data."[39] HTTP headers collect data including "IP addresses, information about the web browser, page location, document, referrer and person using the website."[40] Pixel-specific data includes such data as the "Pixel ID and the Facebook Cookie."[41]

129. Meta Pixel takes the information it harvests and sends it to Facebook with personally identifiable information, such as a user's IP address, name, email, phone number, and specific Facebook ID. Anyone who has access to this Facebook ID can use this identifier to quickly and easily locate, access, and view a user's corresponding Facebook profile. Facebook stores this information on its servers, and, in some instances, maintains this information for years.[42]

130. Facebook has a number of ways to exploit personally identifiable information uniquely forwarded from third-party websites through Meta Pixel.

131. If a user has a Facebook account, the user data collected can be linked to an individual user's Facebook account. For example, if the user is logged into their Facebook account when the user visits a third-party website where the Meta Pixel is installed, many common browsers will attach third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.

---

[39] https://developers.facebook.com/docs/meta-pixel/
[40] https://developers.facebook.com/docs/meta-pixel/
[41] https://developers.facebook.com/docs/meta-pixel/
[42] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

132. Alternatively, Facebook can link the data to a user's Facebook account through the "Facebook Cookie."[43] The Facebook Cookie is a workaround to recent cookie-blocking applications used to prevent websites from tracking users.[44]

133. While the Meta Pixel tool "hashes" personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent *Facebook* from using the data.[45] In fact, Facebook explicitly uses the hashed information to build user profiles.[46]

134. Facebook also receives personally identifiable information in the form of user's unique IP addresses that stay the same as users visit multiple websites. When browsing a third-party website that has embedded Facebook code, a user's IP address is forwarded to Facebook by GET requests, which are triggered by Facebook code snippets. The IP address enables Facebook to keep track of the website page visits associated with that address.

135. Facebook also places cookies on visitors' computers. It then uses these cookies to store information about each user. For example, the "c_user" cookie is a unique identifier that identifies a Facebook user's ID. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

136. The data supplied by the c_user cookie allows Facebook to identify the Facebook account associated with the cookie. One simply needs to log into Facebook, and then type www.facebook.com/#, with the c_user identifier in place of the "#." For example, the c_user cookie for Mark Zuckerberg is 4. Logging into Facebook and typing www.facebook.com/4 in

---

[43] https://clearcode.cc/blog/facebook-first-party-cookie-adtech/
[44] https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/
[45] https://www.facebook.com/business/help/611774685654668?id=120537668283214 2
[46] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

137. Similarly, the "lu" cookie identifies the last Facebook user who logged in using a specific browser. Like IP addresses, cookies are included with each request that a user's browser makes to Facebook's servers. Facebook employs similar cookies such as "datr," "fr," "act," "presence," "spin," "wd," "xs," and "fbp" cookies to track users on websites across the internet.[47] The fbp cookie, for example, is a Facebook identifier that is set by Facebook source code and associated with Defendant's use of the Facebook Tracking Pixel program. The fbp cookie emanates from Defendant's web properties but is transmitted to Facebook through cookie synching technology that Facebook employs. These cookies allow Facebook to easily link the browsing activity of its users to their real-world identities, and such highly sensitive data as medical information, religion, and political preferences.[48]

138. Facebook also uses browser fingerprinting to uniquely identify individuals. Web browsers have several attributes that vary between users, like the browser software system, plugins that have been installed, fonts that are available on the system, the size of the screen, color depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The likelihood that two browsers have the same fingerprint is at least as low as 1 in 286,777, and the accuracy of the fingerprint increases when combined with cookies and the user's IP address. Facebook recognizes a visitor's browser fingerprint each time a Facebook button is loaded on a third-party website page. Using these various methods, Facebook can identify individual users, watch as they browse third-party websites like www.capitalhealth.org, and target users with advertising based on their web activity.

---

[47] https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a#:~:text=browser%20session%20ends.-,%E2%80%9Cdatr%E2%80%9D,security%20and%20site%20integrity%20features.

[48] https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf

139. Facebook then sells advertising space by highlighting its ability to target users. Facebook can target users so effectively because it surveils user activity both on and off its official website. This allows Facebook to make inferences about users far beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[49] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to create highly specific targeted advertising. Indeed, Facebook utilizes precisely the type of personal health information that Defendant bartered to Facebook so that Facebook can identify, target, and market products and services to individuals.

D. Defendant discretely embedded the Meta Pixel tool on its website, resulting in the capture and disclosure of patients' protected health information to Facebook.

140. A third-party website that incorporates Meta Pixel benefits from the ability to analyze a user's experience and activity on the website to assess the website's functionality and traffic. The third-party website also gains information from its customers through Meta Pixel that can be used to target them with advertisements, as well as to measure the results of advertising efforts.

141. Facebook's intrusion into the personal data of visitors to third-party websites incorporating the Meta Pixel is both significant and unprecedented. When Meta Pixel is incorporated into a third-party website, unbeknownst to users and without their consent, Facebook gains the ability to surreptitiously gather every user interaction with the website ranging from what the user clicks on to the personal information entered on a website search bar. Facebook aggregates this data against all websites visited by a specific user.[50] Facebook benefits from obtaining this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users with ads.

---

[49] https://www.facebook.com/business/ads/ad-targeting
[50] https://www.facebook.com/business/help/742478679120153?id=1205376682832142

142. Facebook provides websites using Meta Pixel with the data it captures in the "Meta Pixel page" in Events Manager, as well as tools and analytics to reach these individuals through future Facebook ads.[51] For example, websites can use this data to create "custom audiences" to target the specific Facebook user, as well as other Facebook users who match "custom audience's" criteria.[52] Businesses that use Meta Pixel can also search through Meta Pixel data to find specific types of users to target, such as men over a certain age.

143. Businesses install the Meta Pixel software code to help drive and decode key performance metrics from visitor traffic to their websites.[53] Businesses also use the Meta Pixel to build custom audiences on Facebook that can be used for their own advertising purposes.[54]

144. For example, when a user on many hospital websites clicks on a "Schedule Online" button next to a doctor's name, Meta Pixel sends the text of the button, the doctor's name, and the search term (such as "cardiology") used to find the doctor to Facebook. If the hospital's website has a drop-down menu to select a medical condition in connection with locating a doctor or making an appointment, that condition is also transmitted to Facebook through Meta Pixel.

145. Facebook has designed the Meta Pixel such that Facebook receives information about patient activities on hospital websites as they occur in real time. Indeed, the moment that a patient takes any action on a webpage that includes the Meta Pixel—such as clicking a button to register, login, or to create an appointment—Facebook code embedded on that page sends the content of the patient's communications to Facebook while the exchange of information between the patient and hospital is still occurring.

---

[51] https://www.facebook.com/business/help/742478679120153?id=1205376682832142
[52] https://developers.facebook.com/docs/marketing-api/reference/custom-audience/
[53] https://instapage.com/blog/meta-pixel
[54] https://instapage.com/blog/meta-pixel

146. Defendant is among the hospital systems who have embedded Meta Pixel on their websites. Via its use of the Meta Pixel, Defendant intercepted and disclosed the contents of Plaintiffs' and Class Members' communications with Defendant, including the precise text of patient search queries and communications about specific doctors, communications about medical conditions and treatments, and buttons clicked to Search, Find a Doctor, connect, Login, or Enroll in Defendant's patient portal, summaries of Defendant's responsive communications, the parties to the communications, and the existence of communications at Defendant's websites.

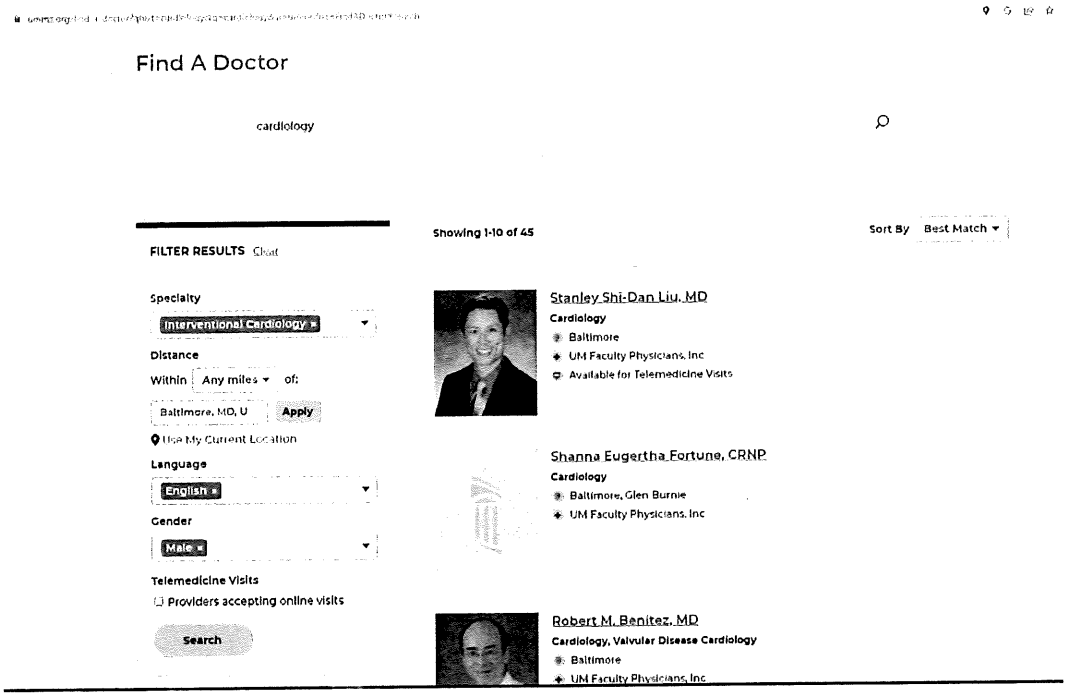
147. For example, when a patient visits the homepage of Defendant's website, the source code employed by Defendant causes personally identifiable information to be transmitted to Facebook.

148. Likewise, when a patient enters their personal information through Defendant's websites that incorporate Meta Pixel, such as to locate a doctor or search for treatment information, these communications, including what the patient is being treated for, are immediately and instantaneously routed to Facebook via the Meta Pixel. The acquisition and disclosure of these communications occurs contemporaneously with the transmission of these communications by patients.

149. This data, which can include sensitive medical information such as medical conditions (e.g., addiction, Alzheimer's, heart disease), diagnoses, procedures, test results, the treating physician, medications, as well as personally identifiable information is obtained and used by Facebook, as well as other third parties.

150. For example, a patient searching for a doctor on Defendant's website located at www.umms.org is asked to provide information about the specialty they are seeking a doctor for, the city they live in, and their preferred gender. The search criteria entered by prospective

patients then provides them with specific physicians who can provide the requested services:

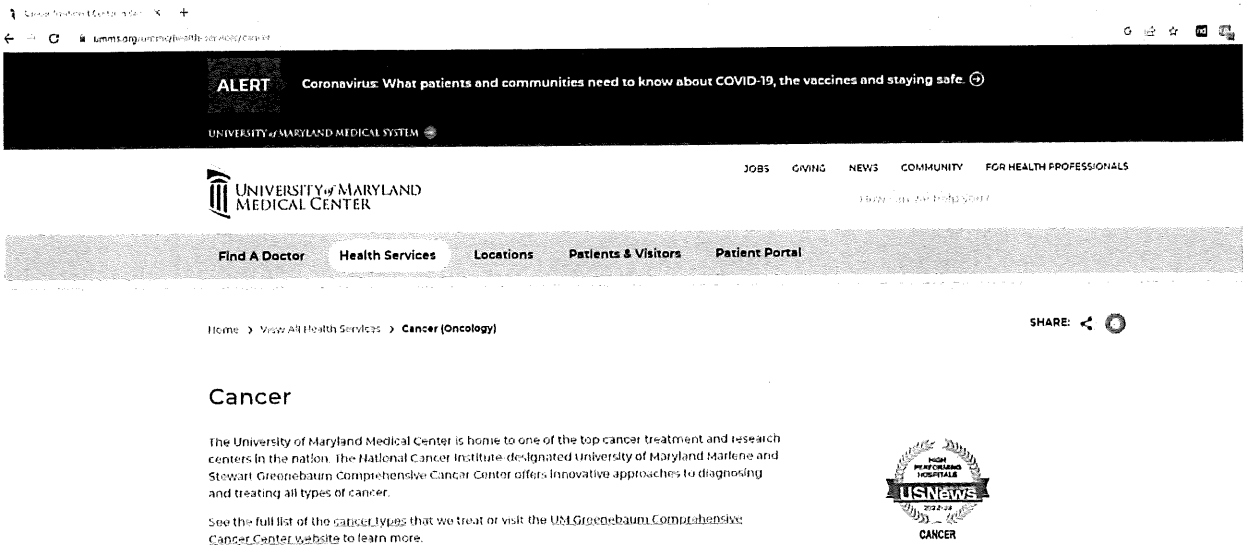


151. All this data about the medical treatments that patients are seeking is disclosed to Facebook simultaneously in real time as patients transmit their information, along with other data, such as patient's unique Facebook ID that is captured by the c_user cookie, which allows Facebook to link this information to patients' unique Facebook accounts. Defendant also discloses other personally identifiable information to Facebook, such as patient IP addresses, URLs, cookie identifiers, browser-fingerprints, device identifiers, and other unique identifying characteristics and/or codes.

152. In other words, Facebook learned not just that patients are seeking treatment, but where and typically when they are seeking treatment, along with other information that patients would reasonably assume that Defendant is not sharing with third party marketing companies.

153. Likewise, Defendant allows patients to search for information about "Health Services" such as "Cancer (Oncology)," "Pregnancy and Childbirth," and "Reconstructive

Plastic Surgery."[55] A patient searching for information about cancer treatment or pregnancy, however, not only shares their personal data with Defendant but also unknowingly shares their personal data with Facebook such as the fact that they have cancer:



154. Defendant discloses patient information from across its website including (but not limited to) communications that are captured by the website's search bar, communications that are captured when a patient searches for information about classes such as "Childbirth" and "Breastfeeding," communications made by patients using the website's Bill Pay/Financials function, and communications made when patients are researching specific medical conditions such as COVID-19. Defendant also makes similar disclosures to Facebook, Google, and other third parties when patients click on the "Log in" buttons of the password protected portions of its website, including its patient portal and bill pay functions, confirming to these companies that the website users are UMMC patients.

[55] https://www.umms.org/ummc/health-services

155. As the above demonstrates, knowing what information a patient is reviewing on Defendant's website can reveal deeply personal and private information. For example, a simple search for "pregnancy" on Defendant's website tells Facebook that the patient is likely pregnant. Indeed, Facebook might know that the patient is pregnant before the patient's close family and friends. But there is nothing visible on Defendant's website that would indicate to patients that, when they use Defendant's search function, their personally identifiable data and the precise content of their communications with Defendant are being automatically captured and made available to Facebook, who can then use that information for advertising purposes even when patients search for treatment options for sensitive medical conditions such as cancer or substance abuse.

156. The amount of data collected is significant. Via the Meta Pixel, when patients interact with its website, Defendant discloses a full-string, detailed URL to Facebook, which contains the name of the website, folder and sub-folders on the webserver, and the name of the precise file requested. For example, when a patient types a search term into the search bar on Defendant's website, the website returns links to information relevant to the search term. When patients then click these links, a communication is created that contains a GET request and a full-string detailed URL.

157. Facebook's Meta Pixel collects and forwards this data to Facebook, including the full referral URL (including the exact subpage of the precise terms being reviewed) and Facebook then correlates the URL with the patient's Facebook user ID, time stamp, browser settings, and even the type of browser used. In short, the URLs, by virtue of including the particular document within a website that a patient views, reveal a significant amount of personal data about a patient. The captured search terms and the resulting URLs divulge a patient's

medical issues, personal interests, queries, and interests on third-party websites operating outside of Facebook's platform.

158. The transmitted URLs contain both the "path" and the "query string" arising from patients' interactions with Defendant's websites. The path identifies where a file can be found on a website. For example, a patient reviewing information about the "Services" that Defendant offers patients such as "Pregnancy and Childbirth" will generate a URL with the path https://www.umms.org/ummc/health-services/womens-health/obstetrics-gynecology/pregnancy-childbirth.

159. Likewise, a query string provides a list of parameters. An example of a URL that provides a query string is https://www.umms.org/ummc/search?q=HIV. The query string parameters in this search indicate that a search was done at Defendant's website for information about HIV. In other words, the Meta Pixel captures information that connects a particular user to a particular healthcare provider.

160. Defendant also provides Facebook with details about online forms that patients fill out in the form of POST requests, such as when a patient utilizes the UMMC website's "Find A Doctor" function. All the information that patients provide when filling out these forms are also disclosed to Facebook.

161. The contents of patients' search terms shared with Facebook plainly relate to (and disclose) the past, present, or future physical or mental health or condition of individual patients who interact with Defendant's website. Worse, no matter how sensitive the area of the Defendant's website that a patient reviews, the referral URL is acquired by Facebook along with other personally identifiable information.

162. The nature of the collected data is also important. Defendant's unauthorized disclosures result in Facebook obtaining a comprehensive browsing history of an individual patient, no matter how sensitive the patient's medical condition. Facebook is then able to correlate that history with the time of day and other user actions on Defendant's website. This process results in Facebook acquiring a vast repository of personal data about patients—all without their knowledge or consent.

163. Defendant also discloses the same kind of patient data described above to other third parties involved in internet marketing, including Google, DoubleClick Digital Marketing, and ShareThis via tracking software that Defendant has installed on its website. As with the Facebook Meta Pixel, Defendant provides patients and prospective patients with no notice that Defendant is disclosing the contents of their communications to these third parties. Likewise, Defendant does not obtain consent from patients and prospective patients before forwarding their communications to these companies.

164. These disclosures to third parties other than Facebook are equally disturbing. Google Analytics, for example, has been described by the Wall Street Journal as "far and away the web's most dominant analytics platform," which "tracks you whether or not you are logged in."[56] Like Facebook, Google tracks internet users with IP addresses, cookies, geolocation, and other unique device identifiers. Defendant routinely discloses patients' personal health information to such Google services as Google Analytics, Google DoubleClick, and Google AdWords.

165. Google cookies provide personally identifiable data about patients who visit Defendant's website to Google. Defendant transmits personally identifiable Google cookie data to Google.

[56] https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401

166. Google warns web-developers that Google marketing tools are not appropriate for health-related webpages and websites. Indeed, Google warns web developers that "Health" is a prohibited category that should not be used by advertisers to target ads to users or promote advertisers' products or services.

167. Defendant deploys Google tracking tools on nearly every page of its websites, resulting in the disclosure of communications exchanged with patients to be transmitted to Google. These transmissions occur simultaneously with patients' communications with Defendant and include communications that Plaintiff and Class Members made about specific medical providers, treatments, conditions, appointments, payments, and registrations and logins to Defendant's patient portal.

168. By compelling visitors to its websites to disclose personally identifiable data and sensitive medical information to Facebook and other third parties, Defendant knowingly disclosed information that allowed Facebook and other advertisers to link its patients' personal health information to their private identities and target them with advertising. Defendant intentionally shared the personal health information of its patients with Facebook in order to gain access to the benefits of the Meta Pixel tool.

169. Defendant facilitated the disclosure of Plaintiff Jane Doe's Personal Health information, including sensitive medical information, to Facebook without her consent or authorization when she entered information on the websites that Defendant maintains.

170. For example, Plaintiff Jane Doe is an individual who has maintained a Facebook account since 2006 and who has also been a patient of UMMC. Jane Doe visited Defendant's website as recently as December 2021 at www.umms.org and entered data, including sensitive medical information, such as details about her medical condition and doctor. The information

that Plaintiff Jane Doe transmitted included, among other things, queries related to her pregnancy and post-partum follow-up.

171. This information could then be combined with other information in Facebook's possession, like her name, date of birth, and phone number, to target Plaintiff more effectively with advertisements or to sell Plaintiff's data to third parties.

172. Because Defendant embedded the Meta Pixel on its website, Defendant disclosed intimate details about Plaintiff's interactions with its website, including Plaintiff's scrolling, typing, and selecting options from drop down menus. Each time the Meta Pixel was triggered, it caused Plaintiff's information to be secretly transmitted to Facebook's servers, as well as additional information that captures and discloses the communications' content and Plaintiff's identity. For example, when Plaintiff and Class Members visited Defendant's website, their personal health information was transmitted to Facebook, including such engagement as using the website's search bar, using the website's Find a Doctor function, and typing content into online forms. During these same transmissions, Defendant's website would also provide Facebook with Plaintiff's and Class Members' Facebook ID, IP addresses, device IDs, and other information that Plaintiff and Class Members provided. This is precisely the type of information that state and federal law require healthcare providers to de-identify to protect the privacy of patients.

173. Plaintiff Jane Doe believed that her interactions with Defendant's website were private and would not be shared with anyone besides her health care providers and their staff. Plaintiff Jane Doe was dismayed when she learned that her personal health information had been sent to Facebook without her consent.

174. Defendant knew that by embedding Meta Pixel—a Facebook advertising tool—it was permitting Facebook to collect, use, and share Plaintiff's and the Class Members' personal health information, including sensitive medical information and personally identifiable data. Defendant was also aware that such information would be shared with Facebook simultaneously with patients' interactions with its websites. Defendant made the decision to barter its patients' Personal Health Care Information to Facebook because it wanted access to the Meta Pixel tool. While that bargain may have benefited Defendant and Facebook, it also betrayed the privacy rights of Plaintiff and Class Members.

F. Plaintiff and the Class Members did not consent to the interception and disclosure of their protected health information.

175. Plaintiff and Class Members had no idea when they interacted with Defendant's websites that their personal data, including sensitive medical data, was being collected and simultaneously transmitted to Facebook. That is because, among other things, Meta Pixel is secretly and seamlessly integrated into Defendant's websites and is invisible to patients visiting those websites.

176. For example, when Plaintiff Jane Doe visited Defendant's website at www.umms.org there was no indication that the Meta Pixel was embedded on that website or that it would collect and transmit her sensitive medical data to Facebook.

177. Plaintiff and her fellow Class Members could not consent to Defendant's conduct when there was no indication that their sensitive medical information would be collected and transmitted to Facebook in the first place.

178. While Defendant purports to have a privacy policy, that privacy policy is effectively hidden from patients. There is no link to Defendant's privacy policy on the homepage of Defendant's website. Nor does Defendant provide any easy way to locate its

privacy policy on its website. Instead, the only way that a patient or potential patient visiting Defendant's website could locate Defendant's privacy policy clicking through multiple screens and links until the user locates Defendant's "Notice of Privacy Practices."[57]

179. Even if a patient stumbled upon Defendant's "Notice of Practices," nothing in that notice would be understood by any reasonable patient to mean that Defendant is routinely allowing Facebook to capture and exploit patients' personal health information.

180. Defendant's "Notice of Privacy Practices" gives no indication to patients that Defendant routinely allows Facebook to capture and exploit patients' personal health information. Defendant assures patients that it is "required by to maintain the privacy and security of your protected health information."[58] This statement is false, deceptive, and misleading because Defendant, in fact, tracks patients' and potential patients' IP addresses, cookies, browser-fingerprints, and device identifiers, which it then causes the transmission of the same to third parties along with patients' and potential patients' sensitive medical information.

181. Further, Defendant expressly promises that it will *never* disclose patient's personal information for marketing purposes or for sale without patients' express written permission:

> In these cases we never share your information unless you give us written permission:
>
> - Marketing purposes
> - Sale of your information

182. These statements are also false, deceptive, and misleading. As described herein, Defendant routinely shares information with Facebook and Google for marketing purposes.

183. Defendant's privacy policy is also false, deceptive, and misleading because

[57] https://www.umms.org/ummc/about/policies/privacy-policy
[58] https://www.umms.org/ummc/about/policies/privacy-policy

Defendant does in fact routinely sell and/or barter its patients' personal health information to Facebook without patients' knowledge or consent in return for access to the Meta Pixel tool.

184. What's more, the very term "Privacy Policy" is deceptive. Research has consistently shown that a majority of Americans who see that a website has a "Privacy Policy" falsely believe that the company with the policy cannot (and will not) disclose information about them to third parties without their consent.

185. Defendant does not have a legal right to share Plaintiff's and Class Members' Protected Health Information without their written consent to third parties, because this information is protected from such disclosure by law. *See* Md. Ann. HG § 4-302; 45 C.F.R. § 164.508. Nor is Defendant permitted to disclose patients' Protected Health Information to advertising and marketing companies like Facebook without express written authorization from patients. *Id.*

186. Defendant failed to obtain a valid written authorization from Plaintiff or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications for marketing purposes. Moreover, no *additional* privacy breach by Facebook is necessary for harm to have accrued to Plaintiff and Class Members; the secret disclosure by Defendants of its patients' personal health information to Facebook means that a significant privacy injury has *already occurred.*

187. Likewise, a patient's reasonable expectation that their health care provider will not share their information with third parties for marketing purposes is not subject to waiver via an inconspicuous privacy policy hidden away on a company's website. Further, Defendant expressly promised its patients that it would never sell or use their personal health information for marketing purposes without express authorization.

188. Defendant violated its own privacy policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' personal health information to Facebook and other third parties without disclosing such activity and without obtaining patients' written consent to share such information.

189. Accordingly, Defendant lacked authorization to intercept, collect, and disclose Plaintiff and Class Members' personal health information to Facebook or aid in the same.

G. Defendant's disclosures of personal patient data to Facebook are unnecessary.

190. There is no information anywhere on the websites operated by Defendant that would alert patients that their most private information (such as their identifiers, their medical conditions, and their medical providers) is being automatically transmitted to Facebook. Nor are any of the disclosures of patient personal health information to Facebook necessary for Defendant to maintain its healthcare website or provide medical services to patients.

191. For example, it is possible for a healthcare website to provide a doctor search function without allowing disclosures to third-party advertising companies about patient sign ups or appointments. It is also possible for a website developer to utilize tracking tools without allowing disclosure of patients' Personal Healthcare Information to companies like Facebook. Likewise, it is possible for Defendant to provide medical services to patients without sharing their personal health information with Facebook so that this information can be exploited for advertising purposes.

192. Despite these possibilities, Defendant willfully chose to implement Meta Pixel on its websites and aid in the disclosure of personally identifiable information and sensitive medical information about its patients, as well as the contents of their communications with Defendant, to third-parties, including Facebook.

H. Plaintiff and Class Members have a reasonable expectation of privacy in their personal health information, especially with respect to sensitive medical information.

193. Plaintiff and Class Members have a reasonable expectation of privacy in their personal health information, including personally identifiable data and sensitive medical information. Defendant's surreptitious interception, collection, and disclosure of patients' personal health information to Facebook violated Plaintiff and Class Member's privacy interests.

194. As patients, Plaintiffs had a reasonable expectation of privacy that their health care provider and its associates would not disclose their personal health information to third parties without their express authorization.

195. The original Hippocratic Oath, circa 400 B.C., provided that physicians must pledge, "What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of man, which on no account must be spread abroad, I will keep to myself holding such things shameful to be spoken about."[59]

196. The modern Hippocratic Oath provides, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."[60] Likewise, the American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications. For example, the AMA has issued medical ethics opinions providing that "[p]rotecting information gathered in association with the care of a patient is a core value in health care. However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust....Physicians must seek to protect patient privacy in all settings to the greatest extent possible and should ... [m]inimize intrusion on privacy when the patient's privacy must be

[59] *Brandt v. Medical Defense Associates*, 856 S.W.2d 667, 671 n.1 (Mo. 1993).
[60] https://www.pbs.org/wgbh/nova/doctors/oath_modern.html

balanced against other factors [and inform] the patient when there has been a significant infringement on privacy of which the patient would otherwise not be aware."[61]

197. The AMA's ethics opinions have further cautioned physicians and hospitals that "[d]isclosing information to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship." [62]

198. Patient personal health information is specifically protected by law. *See* Md. Ann. HG § 4-302; CL § 14-3502; CL § 14-3508. The prohibitions against disclosing patient personal health information include prohibitions against disclosing personally identifiable information such as patient names, IP addresses, and other unique characteristics or codes. *See* Md. Ann. CL § 14-3503; 45 C.F.R. § 164.514. Both state and federal law also restrict the use of patients' Personal Health information, including their status as patients, to only those uses related to their care unless patients have provided express written authorization to the contrary.

199. Maryland has long recognized that physicians owe a duty of confidentiality to patients, which prohibits them from disclosing patients' health information without patients' written consent. *Warner v. Lerner*, 348 Md. 733, 740–41 (1998). This legal framework applies to health care providers, such as Defendant.

200. Plaintiffs' and Class Members' reasonable expectations of privacy in their personal health information are grounded in, among other things, Defendant's status as a health care provider, Defendant's common law obligation to maintain the confidentiality of patients' personal health information, state and federal laws protecting the confidentiality of medical

[61] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (opinion 3.1.1).
[62] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (opinion 3.2.4).

information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendant's express and implied promises of confidentiality.

201. It was reasonable for Plaintiffs and Class Members to assume that Defendant's privacy policies were consistent with Defendant's duties to protect the confidentiality of patients' personal health information.

202. Indeed, multiple studies examining the collection and disclosure of consumers' sensitive medical information confirm that the disclosure of sensitive medical information violates expectations of privacy that have been established as general social norms.

203. Privacy polls and studies also uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

204. For example, a recent study by *Consumer Reports* showed that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believed that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[63]

205. Users act consistently with these preferences. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.[64]

206. The concern about sharing personal medical information is compounded by the

[63] https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/
[64] https://www.wired.co.uk/article/apple-ios14-facebook

reality that advertisers view this type of information as particularly valuable. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one recent article noted, "What is particularly worrying about this process of datafication of children is that companies like [Facebook] are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[65]

207. Many privacy law experts have expressed serious concerns about patients' sensitive medical information being disclosed to third-party companies like Facebook. As those critics have pointed out, having a patient's personal health information disseminated in ways the patient is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

I. Plaintiff's Personal Health Data that Defendant collected, disclosed, and used is Plaintiff's property, has economic value, and its illicit disclosure has caused Plaintiff harm.

208. It is common knowledge that there is an economic market for consumers' personal data—including the kind of data that Defendant has collected and disclosed from Plaintiff and Class Members.

209. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender and location information" were being sold for approximately "$0.50 per 1,000 people."[66]

210. In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about

[65] https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/
[66] https://ig.ft.com/how-much-is-your-personal-data-worth/

"$0.30" per name.[67] That same article noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge" and that the value of a single user's data can vary from $15 to more than $40 per user.[68]

211. In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that consumers "should think of Facebook's cost as [their] data and scrutinize the power it has to set its own price."[69] This price is only increasing. According to Facebook's own financial statements, the value of the average American's data in advertising sales rose from $19 to $164 per year between 2013 and 2020.[70]

212. Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.[71]

213. Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings,[72] and has paid teenagers and adults up to $20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.[73]

---

[67] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/
[68] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/
[69] https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/
[70] https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/
[71] https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/; *see also https://slate.com/technology/2022/06/health-data-brokers-privacy.html*
[72] https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounciations-app
[73] https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html

214. A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.[74]

215. Given the monetary value that data companies like Facebook have already paid for personal information in the past, Defendant has deprived Plaintiff and the Class Members of the economic value of their sensitive medical information by collecting, using, and disclosing that information to Facebook and other third parties without consideration for Plaintiff and the Class Member's property.

J. Defendant is enriched by making unlawful, unauthorized, and unnecessary disclosures of its patients' protected health information.

216. In exchange for disclosing personal health information about its patients, Defendant is compensated by Facebook with enhanced online advertising services, including (but not limited to) retargeting and enhanced analytics functions.

217. Retargeting is a form of online targeted advertising that targets users with ads based on their previous internet actions, which is facilitated through the use of cookies and tracking pixels. Once an individual's data is disclosed and shared with a third-party marketing company, the advertiser is able to show ads to the user elsewhere on the internet.

218. For example, retargeting could allow a web-developer to show advertisements on other websites to customers or potential customers based on the specific communications exchanged by a patient or their activities on a website. Using the Meta Pixel, a website could target ads on Facebook itself or on the Facebook advertising network. The same or similar advertising can be accomplished via disclosures to other third-party advertisers and marketers.

219. Once personally identifiable information relating to patient communications is disclosed to third parties like Facebook, Defendant loses the ability to control how that

[74] https://www.creditdonkey.com/best-apps-data-collection.html; *see also https://www.monetha.io/blog/rewards/earn-money-from-your-data/*

information is subsequently disseminated and exploited.

220. The monetization of the data being disclosed by Defendant, both by Defendant and Facebook, demonstrates the inherent value of the information being collected.

K. Facebook's history of egregious privacy violations.

221. Defendant knew or should have known that Facebook could not be trusted with its patients' sensitive medical information.

222. Due to its ability to target individuals based on granular data, Facebook's ad-targeting capabilities have frequently come under scrutiny. For example, in June 2022, Facebook entered into a settlement with the Department of Justice regarding its Lookalike Ad service, which permitted targeted advertising by landlords based on race and other demographics in a discriminatory manner. That settlement, however, reflected only the latest in a long history of egregious privacy violations by Facebook.

223. In 2007, when Facebook launched "Facebook Beacon," users were unaware that their online activity was tracked, and that the privacy settings originally did not allow users to opt-out. As a result of widespread criticism, Facebook Beacon was eventually shut down.

224. Two years later, Facebook made modifications to its Terms of Service, which allowed Facebook to use anything a user uploaded to its site for any purpose, at any time, even after the user ceased using Facebook. The Terms of Service also failed to provide for any way for users to completely delete their accounts. Under immense public pressure, Facebook eventually returned to its prior Terms of Service.

225. In 2011, Facebook settled charges with the Federal Trade Commission relating to its sharing of Facebook user information with advertisers, as well as its false claim that third-party apps were able to access only the data they needed to operate when—in fact—the apps

could access nearly all of a Facebook user's personal data. The resulting Consent Order prohibited Facebook from misrepresenting the extent to which consumers can control the privacy of their information, the steps that consumers must take to implement such controls, and the extent to which Facebook makes user information available to third parties.[75]

226. Facebook found itself in another privacy scandal in 2015 when it was revealed that Facebook could not keep track of how many developers were using previously downloaded Facebook user data. That same year, it was also revealed that Facebook had violated users' privacy rights by harvesting and storing Illinois' users' facial data from photos without asking for their consent or providing notice. Facebook ultimately settled claims related to this unlawful act for $650 million.[76]

227. In 2018, Facebook was again in the spotlight for failing to protect users' privacy. Facebook representatives testified before Congress that a company called Cambridge Analytics may have harvested the data of up to 87 million users in connection with the 2016 election. This led to another FTC investigation in 2019 into Facebook's data collection and privacy practices, resulting in a record-breaking five-billion-dollar settlement.

228. Likewise, a different 2018 report revealed that Facebook had violated users' privacy by granting access to user information to over 150 companies.[77] Some companies were even able to read users' private messages.

229. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[78] This failure to protect users' data enabled thousands of

[75] https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter
[76] A similar case is pending in Texas.
[77] https://www.cnbc.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html
[78] https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/

developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

230. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective … at preventing the receipt of sensitive data."[79]

231. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data is not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[80] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[81]

[79] https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf
[80] https://slate.com/technology/2022/06/health-data-brokers-privacy.html
[81] https://slate.com/technology/2022/06/health-data-brokers-privacy.html

232. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose."[82]

233. These revelations were confirmed by an article published by the Markup on June 16, 2022, which found during the course of its investigation that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[83]

234. Despite knowing that the Meta Pixel code embedded in its websites was sending patients' personal health information to Facebook, Defendant did nothing to protect its patients from egregious intrusions into its patients' privacy, choosing instead to benefit at those patients' expense.

L. Defendant's failure to inform its patients that their personal health information has been disclosed to Facebook or to take steps to halt the continued disclosure of such information is malicious, oppressive, and in reckless disregard of Plaintiff's and Class Members' rights.

235. Hospital systems, like other businesses, have a legal obligation to disclose data breaches to their customers. Md. Com. Law §14-3504(h).

---

[82] https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes
[83] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

236. After publication of the Markup's investigative article in June 2022, hospital systems around the United States began self-reporting data breaches arising from their installation of pixel technology on their websites.[84]

237. For example, in August 2022, Novant Health informed approximately 1.3 million patients that their medical data was disclosed to Facebook due to the installation of the Facebook Meta Pixel on the hospital system's websites.[85] Novant Health's data breach announcement conceded that the Meta Pixel tool installed on its websites "allowed certain private information to be transmitted to Meta from the Novant Health website."[86] Novant Health further admitted that the information about its patients that was disclosed to Facebook included "an impacted patient's: demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes."[87]

238. Likewise, in October 2022, Advocate Aurora Health informed approximately 3 million patients that their personal health information had been disclosed to Facebook via the Meta Pixel installed on Advocate Aurora Health's website.[88]

239. Advocate Aurora Health's data breach notification conceded that patient information had been transmitted to third parties including Facebook and Google when patients used the hospital system's website.[89]

---

[84] https://www.scmagazine.com/analysis/breach/pixel-fallout-expands-community-health-informs-1-5m-of-unauthorized-disclosure

[85] https://www.scmagazine.com/analysis/breach/1-3m-novant-health-patients-notified-of-unintended-disclosure-via-facebook-pixel

[86] https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx

[87] https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx

[88] https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3

240. Advocate Aurora Health further admitted that a substantial amount of its patients' personal health information has been shared with Facebook and Google including patients' "IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; [and] type of appointment or procedure."[90] Even more troubling, Advocate Aurora Health admitted that "[w]e cannot confirm how vendors used the data they collected."[91]

241. Advocate Aurora Health claimed that, in conjunction with its data breach notice, the hospital system had "disabled and/or removed the pixels from our platforms and launched an internal investigation to better understand what patient information was transmitted to our vendors."[92] Advocate Aurora Health also promised its 3 million patients that the company had instituted an "enhanced, robust technology vetting process" to prevent such disclosures of its patients' personal health information in the future.[93]

242. Similarly, in October 2022, WakeMed notified more than 495,000 patients that their personal health information had been transmitted to Facebook through the use of tracking pixels installed on its websites.[94] In announcing this data breach, WakeMed admitted that the Facebook Meta Pixel tool had been installed on its website resulting in the transmission of patient information to Facebook.[95] WakeMed further admitted that "[d]epending on the user's activity, the data that may have been transmitted to Facebook could have included information such as: email address, phone number, and other contact information; computer IP address; emergency contact information; information provided during online check-in, such as allergy or

[89] https://www.advocateaurorahealth.org/
[90] https://www.advocateaurorahealth.org/pixel-notification/faq
[91] https://www.advocateaurorahealth.org/pixel-notification/faq
[92] https://www.advocateaurorahealth.org/pixel-notification/faq
[93] https://www.advocateaurorahealth.org/pixel-notification/faq
[94] https://healthitsecurity.com/news/wakemed-faces-data-breach-lawsuit-over-meta-pixel-use
[95] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

medication information; COVID vaccine status; and information about an upcoming appointment, such as appointment type and date, physician selected, and button/menu selections."[96]

243. WakeMed also conceded that it had no idea what Facebook had done with the personal health information that WakeMed had disclosed about its patients.[97] Like other the other hospital systems who have come clean about their use of the Meta Pixel tool, WakeMed promised its patients that it had "proactively disabled Facebook's pixel" and had "no plans to use it in the future without confirmation that the pixel no longer has the capacity to transmit potentially sensitive or identifiable information."[98]

244. In November 2022, the fallout from hospital systems' use of the Meta Pixel tool expanded when Community Health Network informed 1.5 million of its patients that their personal health information had been routinely transmitted and disclosed to Facebook since at least April 2017.[99]

245. In its data breach notice, Community Health admitted that it had "discovered through our investigation that the configuration of certain technologies allowed for a broader scope of information to be collected and transmitted to each corresponding third-party tracking technology vendor (e.g., Facebook and Google) than Community had ever intended." Community Health further conceded that its use of the Meta Pixel and related third-party tracking technologies had resulted in surreptitiously recording and transmitting a wide range of patient engagements with its websites, including "includes scheduling an appointment online or

---

[96] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

[97] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

[98] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

[99] https://healthitsecurity.com/news/community-health-network-notifies-1.5m-of-data-breach-stemming-from-tracking-tech; *see also* https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach

directly with a provider" and "seeking treatment at a Community or affiliated provider location."[100]

246. Community Health, like WakeMed, Novant, and Advocate Aurora Health, also promised its patients that it had disabled or removed the third-party tracking technologies that it had installed on its website and had instituted new "evaluation and management processes for all website technologies moving forward."[101] Community Health, however, also conceded that it had no idea how Facebook or other third parties had exploited the patient personal health information that had been disclosed to them via the pixel technology.

247. Unlike Community Health, WakeMed, Novant, Advocate Aurora Health, and other responsible hospital systems who have informed their patients of the serious privacy violations resulting from the installation of Facebook's Meta Pixel tool on their websites, Defendant has done nothing. Indeed, not only has Defendant hidden these privacy violations from its patients, but Defendant continues to collect, transmit, and disclose its patients' personal health information to Facebook despite widespread knowledge in the health care community that such collection and disclosure of patient personal health information is patently illegal and in violation of patient's fundamental privacy rights.

248. As these data breach announcements demonstrate, there is widespread knowledge within the health care community that installation of the Meta Pixel tool on hospital websites results in the disclosure of patients' personal health information Facebook. There is also widespread recognition that such disclosures are not only illegal but fundamentally unethical, given the privacy rights involved.

[100] https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach
[101] https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach

249. Defendant's decision to hide its use of the Meta Pixel tool from its own patients and its refusal to remove such technologies from its websites even after learning that its patients' personal health information was being routinely collected, transmitted, and exploited by Facebook is malicious, oppressive, and in reckless disregard of Plaintiffs' and Class Members' rights.

TOLLING, CONCEALMENT, AND ESTOPPEL

250. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

251. Defendant seamlessly incorporated Meta Pixel and other trackers into its websites, providing no indication to users that they were interacting with a website enabled by Meta Pixel. Defendant had knowledge that its websites incorporated Meta Pixel and other trackers yet failed to disclose that by interacting with Meta-Pixel enabled websites that Plaintiff and Class Members' sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook.

252. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendants' conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel.

253. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Defendant's illegal interception and disclosure of patients' personal health information has continued unabated through the date of the filing of Plaintiff's Original Complaint. What's more, Defendant was under a duty to disclose the nature and significance of its data collection practices but did not do so. Defendant is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

254. Plaintiff re-alleges and incorporates by reference the allegations as set forth above.

255. Defendant's conduct violates the law and breaches its express and implied privacy promises.

256. Defendant's unlawful conduct has injured Plaintiff and Class Members.

257. Defendant's conduct is ongoing.

258. Plaintiff brings this action individually and as a class action against Defendant.

259. Plaintiff seeks class certification for the following proposed Class:

> **The University of Maryland Medical Center Class:** During the fullest period allowed by law, all current Maryland citizens who are, or were, patients of UMMC or any of its affiliates and who exchanged communications at Defendant's websites, including www.umms.org and any other UMMC affiliated website, including UMMC's patient portal.

260. Excluded from the proposed Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) the Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendant or its parent has a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendant's counsel.

261. Plaintiff reserves the right to redefine the Class and/or add Subclasses at, or prior to, the class certification stage, in response to discovery or pursuant to instruction by the Court.

262. Plaintiff and the Class Members satisfy the numerosity, commonalty, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 2-231.

263. **Numerosity:** While the exact number of Class Members is unknown to Plaintiff

at this time, the Class, based on information and belief, consists of thousands of people dispersed throughout the State of Maryland, such that joinder of all members is impracticable. Indeed, Defendant treats thousands of inpatients a year, the vast majority of which likely have interacted with Defendant's website. The exact number of Class Members can be determined by review of information maintained by Defendants.

264. **Commonality and Predominance:** There are questions of law and fact common to Class Members and which predominate over any questions affecting only individual members. A class action will generate common answers to the questions below, which are apt to drive resolution:

a. Whether Defendant's acts and practices violated Plaintiff's and Class Members' privacy rights;

b. Whether Defendant's acts and practices violate Md. Ann. Code CJP § 10-402;

c. Whether Defendant's acts and practices violate Md. Ann Code HG § 4-302;

d. Whether Defendant knowingly allowed the surreptitious collection and disclosure of Plaintiff and Class Members' personal health information to Facebook, Google, and other third parites;

e. Whether Defendant's acts and practice were intentional;

f. Whether Defendant profited from disclosures of Plaintiffs' and Class Members' personal health information to third parties;

g. Whether Defendant's acts and practices constitute a breach of the duty of physician-patient confidentiality;

h. Whether Defendant profited from disclosures of patient personal health information to third parties including Facebook and Google;

i. Whether Defendant was unjustly enriched;

j. Whether Defendant's acts and practices harmed and continue to harm Plaintiff and Class Members and, if so, the extent of that injury;

k. Whether Plaintiff and Class Members are entitled to equitable relief including, but not limited to, injunctive relief, restitution, and disgorgement;

l. Whether Plaintiff and Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

m. Whether and to what extent Plaintiffs and Class Members are entitled to attorney's fees and costs.

265. These common questions of law and fact predominate over any questions affecting only the individual Class Members.

266. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

267. **Typicality:** Plaintiff's claims are typical of the claims of other Class Members and Plaintiff have substantially the same interest in this matter as other Class Members. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other members of the Class. Plaintiff's claims arise out of the same set of facts and conduct as all other Class Members. Plaintiff and all Class Members are patients of Defendant who used the websites set up by Defendant for patients and are victims of Defendant's respective unauthorized disclosures to third parties including Facebook. All claims of Plaintiff and Class Members are based on Defendant's wrongful conduct and unauthorized disclosures.

268. **Adequacy of Representation:** Plaintiff is committed to prosecuting this action and has retained competent counsel experienced in litigation of this nature. Plaintiff's claims are coincident with, and not antagonistic to, those of other Class Members she seeks to represent. Plaintiff has no disabling conflicts with Class Members. Accordingly, Plaintiff is an adequate representative of the Class and, along with counsel, will fairly and adequately protect the interests of the Class and any Subclasses.

269. **Superiority:** A class action is the superior method for fair and efficient adjudication of the controversy. Although all Class Members have claims against Defendant, the likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to conduct such litigation. The damages, harm, and other financial detriment suffered individually by Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impractical for Class Members to individually seek redress for Defendant's wrongful conduct. Moreover, serial adjudication in numerous venues is not efficient, timely, or proper. Judicial resources would be unnecessarily depleted by prosecution of individual claims. The prosecution of separate actions by individual Class Members could create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which could establish incompatible standards of conduct for Defendant or adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of the members of the Class Members who are not parties to the adjudications. If a class action is not permitted, Class Members will continue to suffer losses and Defendant's misconduct will continue without proper remedy.

270. In addition to satisfying the prerequisites of Rule 2-231(c)(3), Plaintiff satisfies the requirements for maintaining a class action under Rule 2-231(c)(1) and (c)(2) because (a) the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendant; (b) the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or

impede their ability to protect their interests; (c) Defendant has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief herein appropriate with respect to the proposed Class as a whole; and (d) questions of law or fact common to the members of the class predominate over any questions affecting only individual members, and that a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

271. Plaintiff anticipates no unusual difficulties in the management of this litigation as a class action. The Class is readily ascertainable and direct notice can be provided from the records maintained by Defendant, electronically or by publication, the cost of which is properly imposed on Defendant.

272. For the above reasons, among others, a class action is superior to other available methods for the fair and efficient adjudication of this action.

CAUSES OF ACTION

COUNT I
Interception of Electronic Communications in Violation of Md. Ann. Code, Cts. & Jud. Proc. § 10-402
(On Behalf of Plaintiff and the Class)

273. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

274. Plaintiff brings this claim on behalf of herself and all members of the Class.

275. All conditions precedent to this action have been performed or have occurred.

276. Md. Ann. Code, Cts. & Jud. Proc. § 10-402 prohibits any person from willfully and secretly intercepting the contents of electronic communications through the use of any intercepting device unless given prior authority by all parties to a communication to do so.

277. Any person aggrieved by a violation of Cts. & Jud. Proc. § 10-402 "shall have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use the communications." Md. Ann. Code, Cts. & Jud. Proc. § 10-410.

278. Defendant qualifies as a person under the statute.

279. All alleged communications between Plaintiff or Class Members and Defendant qualify as electronic communications under Maryland law because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

280. "Intercept" under the statute means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Md. Code Ann., Cts. & Jud. Proc. § 10-401(10).

281. An "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." Md. Code Ann., Cts. & Jud. Proc. § 10-401(5)(i).

282. Defendant willfully engaged in and continues to engage in intercepting communications by aiding others (including Facebook) to secretly record the contents of Plaintiff's and Class Members' electronic communications.

283. The intercepting devices used in this case include, but are not limited to:

a. Plaintiff and Class Members' personal computing devices;

b. Plaintiff and Class Members' web browsers;

c. Plaintiff and Class Members' browser-managed files;

d. Facebook's Meta Pixel;

e. Internet cookies;

f. Defendant's computer servers;

g. Third-party source code utilized by Defendant; and

h. Computer servers of third parties (including Facebook) to which Plaintiff and Class Members' communications were disclosed.

284. Under the statute, "contents" when used with respect to any wire, oral, or electronic communication includes "any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication." Md. Code Ann., Cts. & Jud. Proc. § 10-401(4).

285. Defendant willfully aided in, and continues to aid in, the interception of contents in that the data from the communications between Plaintiff and/or Class Members and Defendant that were transmitted to and recorded by the third parties include information which identifies the parties to each communication, their existence, and their contents.

286. Defendant intercepted and disclosed the "contents" of Plaintiff's and Class Members' communications in at least the following forms:

a. The parties to the communications;

b. The precise text of patient search queries;

c. Personally identifiable information such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

d. The precise text of patient communications about specific doctors;

e. The precise text of patient communications about specific medical conditions;

f. The precise text of patient communications about specific treatments;

g. The precise text of patient communications about scheduling appointments with medical providers;

h. The precise text of patient communications about billing and payment;

i. The precise text of specific buttons on Defendant's website(s) that patients click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

j. The precise dates and times when patients click to Log-In on Defendant's website(s);

k. Information that is a general summary or informs third parties of the general subject of communications that Defendant sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information; and

l. Any other content that Defendant has aided third parties in scraping from webpages or communication forms at web properties.

287. Plaintiff and Class Members reasonably expected that their personal health information was not being intercepted, recorded, and disclosed to Facebook and other third parties.

288. No legitimate commercial purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Class Members' personal health information to Facebook. Neither Plaintiff nor Class Members consented to the disclosure of their personal health information by Defendant to Facebook and other third parties. Nor could they have consented, given that Defendant never sought Plaintiff or Class Members' consent., much less

told visitors to its website that their every interaction was being recorded and transmitted to Facebook via the Meta Pixel tool.

289. Plaintiff and Class Members' electronic communications were intercepted during transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their personal health information, including using their sensitive medical information to develop marketing and advertising strategies.

290. Under the statute, aggrieved persons are entitled to recover appropriate injunctive relief and "(1) Actual damages but not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1,000, whichever is higher; (2) Punitive damages; and (3) A reasonable attorney's fee and other litigation costs reasonably incurred."

291. In addition to statutory damages, Defendant's breach caused Plaintiff and Class Members the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the doctor-patient relationship;

c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value.

292. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT II
Breach of Implied In Fact Contract
(On Behalf of Plaintiff and the Class)

293. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

294. Plaintiff brings this claim on behalf of herself and all members of the Class.

295. Defendant promises in its "Notice of Privacy Practices" that Defendant assures visitors to its website that "[w]e are required by law to maintain the privacy and security of your protected health information" and that "[w]e will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[102] Further, Defendant expressly promises that it will *never* disclose patient's personal information for marketing purposes or for sale without patients' express written permission. [103]

296. Defendant solicited and invited Plaintiff and Class Members to provide their Private Health Information on its website as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Health Information to Defendant as part of acquiring Defendant's medical services. Per its contractual, legal, ethical, and fiduciary duties, Defendant was obligated to take adequate measures to protect Plaintiff's and Class Members' personal health information from unauthorized disclosure to third parties such as Facebook. These facts give rise to the inference that Defendant took on obligations outside the plain terms of any express contracts that they may have had with Plaintiff and Class Members.

297. Plaintiff and the Class Members entered into valid and enforceable implied contracts with Defendant when they sought medical treatment from Defendant. Specifically,

[102] https://www.umms.org/ummc/about/policies/privacy-policy
[103] https://www.umms.org/ummc/about/policies/privacy-policy

through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of medical care and treatment, which included an implied agreement for Defendant to retain and protect the privacy of Plaintiff's and Class Members' personal health information.

298. Defendant required and obtained Plaintiff's and Class Members' personal health information as part of the physician-patient relationship, evincing an implicit promise by Defendant to act reasonably to protect the confidentiality of Plaintiff's and Class Members' personal health information. Defendant, through its privacy policies, codes of conduct, company security practices, and other conduct, implicitly agreed that it would safeguard Plaintiff's and Class Members' personal health information in exchange for access to that information and the opportunity to treat Plaintiff and Class Members.

299. Implied in the exchange was a promise by Defendant to ensure that the personal health information of Plaintiff and Class Members in its possession would only be used for medical treatment purposes and would not be shared with third parties such as Facebook without the knowledge or consent of Plaintiff and Class Members. By asking for and obtaining Plaintiff's and Class Members' personal health information, Defendant assented to protecting the confidentiality of that information. Defendant's implicit agreement to safeguard the confidentiality of Plaintiff's and Class Members' personal health information was necessary to effectuate the contract between the parties.

300. Plaintiff and Class Members provided their personal health information in reliance on Defendant's implied promise that this information would not be shared with third parties without their consent.

301. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class Members would provide their personal health information in exchange for the medical treatment and other benefits provided by Defendant (including the protection of their confidential personal and medical information). A portion of the price of each payment that Plaintiff and the Class Members made to Defendant for medical services was intended to ensure the confidentiality of their personal health information.

302. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant would comply with its promises to protect the confidentiality of their personal health information as well as applicable laws and regulations governing the disclosure of such information and that Defendant would not allow third parties to collect or exploit their communications with Defendant without their consent.

303. It is clear by these exchanges that the parties intended to enter into an agreement and mutual assent occurred. Plaintiff and Class Members would not have disclosed their personal health information to Defendant but for the prospect of Defendant's promise of medical treatment and other benefits. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' personal health information if it did not intend to provide them with medical treatment and other benefits.

304. Defendant was therefore required to reasonably safeguard and protect the personal health information of Plaintiff and Class Members from unauthorized disclosure and/or use by third parties.

305. Plaintiff and Class Members accepted Defendant's medical services offer and fully performed their obligations under the implied contract with Defendant by providing their personal health information to Defendant among other obligations. Plaintiff and Class Members

would not have provided and entrusted their personal health information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their personal health information for uses other than the benefits offered by Defendant.

306. Plaintiff and Class Members relied on Defendant's implied promises to safeguard their personal health information to their detriment. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' personal health information from disclosure to Facebook and other third parties.

307. Defendant's failure to implement adequate measures to protect the personal health information of Plaintiff and Class Members and Defendant's intentional disclosure of the same to Facebook violated the purpose of the agreement between the parties: Plaintiff's and Class Members' provision of money and personal health information in exchange for medical services and other benefits.

308. Instead of safeguarding Plaintiff's and Class Members' personal health information, Defendant intentionally shared that information with Facebook thereby breaching the implied contracts it had with Plaintiff and Class Members.

309. Plaintiff and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to operate its websites free of surreptitious collection and exploitation of communications between the parties. Defendant failed to do so. Plaintiff and Class Members would not have purchased medical services from Defendant if they knew that Defendant would share their personal health information with Facebook without their knowledge or written consent.

310. Under the implied contracts, Defendant and/or its affiliated healthcare providers promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' personal health information provided to obtain such healthcare. In exchange, Plaintiff and Class Members agreed to pay money for these services, and to turn over their personal health information through the use of Defendant's websites.

311. Both the provision of medical services healthcare and the protection of Plaintiff and Class Members' Private Health Information were material aspects of these implied contracts.

312. The implied contracts for the provision of medical services—contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Health Information unless they consent—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's published Notice of Privacy Practices.

313. Defendant's express representations, including, but not limited to the express representations found in its Notice of Privacy Practices, memorialize and embody an implied contractual obligation requiring Defendant refrain from aiding or allowing third parties to collect or Plaintiff and Class Members' Private Health Information without consent. By soliciting and acquiring Plaintiff's and Class Members' personal health information Defendant assumed an independent duty to handle Plaintiff's and Class Members' personal health information with due care and consistent with industry standards to prevent the foreseeable harm that arises from a breach of that duty.

314. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Health Information associated with obtaining healthcare private. To customers such as Plaintiff and the Class Members, healthcare that allows third parties to

secretly collect their Private Health Information without consent is fundamentally less useful and less valuable than healthcare that refrains from such practices. Plaintiff and Class Members would not have entrusted their Private Health Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Health Information would be safeguarded and protected or entrusted their Private Health Information to Defendant in the absence of its implied promise to do so.

315. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their Private Health Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, (a) the provision of healthcare and medical services and (b) the protection of their Private Health Information.

316. Plaintiff and the Class Members performed their obligations under the contract when they paid for their healthcare services and provided their Private Health Information.

317. Defendant materially breached its contractual obligation to protect the nonpublic Private Health Information Defendant gathered when it allowed third parties to collect and exploit that information without Plaintiff's and Class Members' consent.

318. Defendant also materially breached its contractual obligation to protect Plaintiff's and Class Members' non-public personal health information when it failed to implement adequate security measures and policies to protect the confidentiality of that information. For example, on information and belief, Defendant (1) failed to implement internal policies and procedures prohibiting the disclosure of patients' personal health information without consent to third-party advertising companies like Facebook, (2) failed to implement adequate reviews of the software code and java script installed on its websites to ensure that patients' personal health

information was not being automatically routed without consent to third party advertising companies like Facebook, (3) failed to provide adequate notice to the public that visitors to its websites risked having their personal health information shared with third party advertising companies like Facebook, (4) failed to take other industry standard privacy protection measures such as providing a "cookie" acceptance button on its website homepages, (5) failed to provide visitors to its websites with a means to opt out of the automatic transfer of data regarding their website interactions to third party advertising companies like Facebook, (6) failed to implement internal policies and educational programs to ensure that Defendants' website managers and coders were familiar with the legal regulations governing the disclosure patient personal health information to third parties, and (7) failed take measures to prevent the automatic transmission of patients' personal health information to third party advertising companies like Facebook.

319. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains, and instead received healthcare and other services that were of a diminished value compared to those described in the contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the healthcare services with data privacy they paid for and the healthcare services they received.

320. As a result of Defendant's material breaches, Plaintiff and Class Members were deprived of the benefit of their bargain with Defendant because they spent more on medical services with Defendant than they would have if they had known that Defendant was not providing the reasonable data security and confidentiality of patient communications that Defendant represented that it was providing in its privacy policies. Defendant's failure to honor

its promises that it would protect the confidentiality of patient communications thus resulted in Plaintiff and Class Members overpaying Defendant for the services they received.

321. The services that Plaintiff and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide, which included Defendant's promise that any patient communications with Defendant would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

322. The medical services that Defendant offers are available from many other health care systems who do protect the confidentiality of patient communications. Had Defendant disclosed that it would allow third parties to secretly collect Plaintiff and Class Members' Private Health Information without consent, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

323. Defendant's conduct in sharing Plaintiff's and Class Members' personal health information with Facebook also diminished the sales value of that information. There is a robust market for the type of information that Plaintiff and Class Members shared with Defendant (which Defendant then shared with Facebook). Indeed, Facebook itself has offered to pay the public to acquire similar information in the past so that Facebook could use such information for marketing purposes. Plaintiff and Class Members were harmed both by the dissemination of their personal health information and by losing the sales value of that information.

324. As a direct and proximate result of these failures, Plaintiff and the Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including, without limitation, the release and disclosure of their Private Health Information, the

loss of control of their Private Health Information, the diminution in value of their personal health information, and the loss of the benefit of the bargain they had struck with Defendant.

325. Plaintiff and the Class Members are entitled to compensatory and consequential damages suffered as a result.

326. Plaintiff and Class Members also face a real and immediate threat of future injury to the confidentiality of their Personal Health information both because such information remains within Defendant's control and because anytime that Plaintiff and/or Class Members interact with Defendant's websites to make appointments, such information about their medical conditions, search for a doctor, or otherwise seek assistance with their medical conditions they risk further disclosure of their personal health information. Plaintiff and the Class Members are therefore also entitled to injunctive relief requiring Defendant to cease all website operations that allow for the third-party capture of Private Health Information.

COUNT III
Unjust Enrichment/Quasi-Contract
(On Behalf of Plaintiff and the Class)

327. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

328. Plaintiff hereby pleads this Count in the alternative to Count II.

329. Plaintiff brings this claim on behalf of herself and all members of the Class.

330. Plaintiff and Class Members conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade

for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Defendant in the form of monetary compensation.

331. Plaintiff and the Class Members would not have used the Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties.

332. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

333. The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

334. Defendant should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT IV
Invasion of Privacy—Unreasonable Intrusion upon the Seclusion of Another (On Behalf of Plaintiff and the Class)

335. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

336. Plaintiff brings this claim on behalf of herself and all members of the Class.

337. Defendant promises in its "Notice of Privacy Practices" that it is "required by to maintain the privacy and security of your protected health information."[104] Further, Defendant

[104] https://www.umms.org/ummc/about/policies/privacy-policy

expressly promises that it will *never* disclose patient's personal information for marketing purposes or for sale without patients' express written permission."[105]

338. These promises by Defendant, coupled with Defendant's legal obligations to protect the confidentiality of patient personal health information, were sufficient to create an expectation of privacy by Plaintiff and Class Members that their personal health information would not be disclosed to third party marketing companies like Facebook without their written permission. In these circumstances, a reasonable person could deem Defendant's deceit and disregard for its patient's privacy interests as both highly offensive and an egregious breach of social norms.

339. Under Maryland law, there is a tortious intrusion on seclusion when there is an intentional intrusion on the solitude, seclusion, or private affairs of another by a means that is unreasonable or highly offensive to a reasonable person.

340. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their personal health information and were accordingly entitled to protection of this information against the acquisition and disclosure of their personal health information by unreasonable means.

341. Defendant owed a duty to Plaintiff and Class Members to protect the confidentiality of their personal health information and not to share such information with Facebook for marketing purposes without the express written consent of Plaintiff and Class Members.

342. Defendant promised Plaintiffs and Class Members in its privacy policy that it would protect their personal health information from unauthorized disclosure to and use by third parties.

---

[105] https://www.umms.org/ummc/about/policies/privacy-policy

343. Defendant obtained Plaintiff's and Class Members' personal health information by falsely promising that it would safeguard the confidentiality of that information and that it would never disclose such information to third parties for marketing purposes without written consent. Because Defendant obtained Plaintiff's and Class Members' personal health information through behavior that is rife with deceit and disregard, a reasonable fact finder could (and likely will) find that Defendant's conduct was highly offensive. By same the token, because Defendant created an expectation of privacy on its website that it then violated, a reasonable fact finder could deem Defendant's behavior both "highly offensive" and an egregious breach of social norms."

344. Plaintiffs and Class Members did not authorize, consent, know about, or take any action to indicate consent to Defendant's conduct alleged herein.

345. Defendant's conduct described herein was intentional.

346. Neither Plaintiff nor Class Members authorized or consented to Defendant sharing their personal health information with Facebook, and Defendant's decision to do so nevertheless violated both Defendant's express promises and its legal obligations to protect the confidentiality of its patients' personal health information.

347. In these circumstances, the unauthorized acquisition, appropriation, and disclosure of Plaintiff's and Class Members' personal health information would be highly offensive to a reasonable person. Defendant's promises that it would never disclose patients' protected health information for marketing purposes without their written consent was sufficient to create a reasonable expectation of privacy with respect to Plaintiff's and Class Members' engagement with Defendant's websites.

348. The intrusion was into subject matter that was private and is entitled to be private. Plaintiff and Class Members disclosed their personal health information to Defendant with the understanding that it would only be used for their medical treatment and that such information would be kept confidential and protected from disclosure to third parties. Plaintiff and Class Members reasonably believed that such information would be kept private and would not be shared with Facebook without their authorization so that Facebook could target them with advertising.

349. The disclosure of Plaintiff's and Class Members' personal health information by Defendant constitutes an unreasonable intrusion upon Plaintiff's and Class Members' seclusion, as to both their persons, their private affairs, and private concerns of a kind that would be highly offensive to a reasonable person.

350. Defendant acted with a knowing mind when it intentionally disclosed Plaintiff and Class Members' personal health information to Facebook. Defendant further invaded Plaintiff's and Class Members' privacy by failing to implement adequate data security measures, despite its obligations to protect patients' personal health information.

351. Acting with knowledge, Defendant had notice and knew that its disclosure of Plaintiff's and Class Members' personal health information would cause injury to Plaintiff and Class Members.

352. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' personal health information was transmitted to Facebook and other third parties without authorization, causing Plaintiff and Class Members to suffer injury, including, at minimum, the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Defendants eroded the essential confidential nature of the doctor-patient and provider-patient relationship; and

c. Defendants took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff and Class Members' knowledge, consent, or authorization and without sharing the benefit of such value.

353. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their personal health information can be accessed, acquired by, appropriated by, disclosed to, used by, and/or viewed by unauthorized third parties.

354. Plaintiff and Class Members have no adequate remedy at law for the injuries that they have suffered (and will continue to suffer) because of Defendant's wrongful practices in that a judgment for money damages will not end the invasion of privacy for Plaintiff and Class Members. Accordingly, Plaintiff and Class Members seek such injunctive relief as the Court deems legal, equitable, and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of herself and all others similarly situated, asks for judgment in her favor, and that the Court enter an order as follows:

a. Certifying the Class and appointing Plaintiffs as the Class's representatives;

b. Appoint the law firms of Bodie, Dolina, Hobbs, Friddell & Grenzer, P.C., Simmons Hanly Conroy, Turke & Strauss, LLP, and Ahmad, Zavitsanos, & Mensing P.C. as class counsel;

c. Finding that Defendant's conduct as alleged herein was unlawful;

d. Awarding such injunctive and other equitable relief as the Court deems just and proper, including enjoining Defendant from making any further disclosure of Plaintiff or Class Members' communications to third parties without the Plaintiff or Class Members' express, informed, and written consent;

e. Awarding statutory damages of $1,000 per Plaintiff and Class Members pursuant to Md. Code Ann., Cts. & Jud. Proc. § 10-410.

f. Imposing a constructive trust against Defendant through which Plaintiff and Class Members can be compensated for any unjust enrichment gained by Defendant;

g. Awarding Plaintiff and Class Members statutory, actual, compensatory, consequential, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

h. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law;

i. Awarding Plaintiff and Class Members reasonable attorney's fees, costs, and expenses;

j. Awarding costs of suit; and

k. Such other and further relief to which Plaintiff and Class Members may be entitled.

Dated: February 21, 2023

Thomas J. Dolina, Bar # 00597
Bodie, Dolina, Hobbs, Friddell & Grenzer, P.C.
305 Washington Avenue, Suite 300
Towson, MD 21204
Telephone: (410) 823-1250
Facsimile: (410) 296-0432
tdolina@bodie-law.com

Jay Barnes*
Eric Johnson*
SIMMONS HANLY CONROY
One Court St.
Alton, IL
jaybarnes@simmonsfirm.com
ejohnson@simmonsfirm.com
Telephone: (800) 479-9533
Facsimile: (618) 259-2251

Foster C. Johnson*
David Warden*
Paul Turkevich*
AHMAD, ZAVITSANOS, & MENSING, P.C.
1221 McKinney Street, Suite 3460
Houston, Texas 77010
(713) 655-1101
fjohnson@azalaw.com
dwarden@azalaw.com
pturkevich@azalaw.com

Samuel J. Strauss*
Raina C. Borrelli*
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

* Motions for Admission to be filed

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF FILING

The undersigned hereby certifies that the foregoing Class Action Complaint has been filed using the Court's electronic case filing system on this 21st day of February 2023.

/s/ Thomas J. Dolina
Thomas J. Dolina